Redes de computadores

Redes de computadores

Sergio Eduardo Nunes

Sumário

Palavras do autor

Olá, caro aluno. Você está prestes a começar a compreender o funcionamento das redes de computadores e o modo como todos aqueles serviços utilizados por milhares de pessoas ao redor do mundo diariamente (tais como sites, serviços de hospedagem de dados, e-mail, servidores de impressão, entre outros) são estruturados e configurados.

O entendimento dos aspectos técnicos e das características das redes de computadores proporciona ao profissional de tecnologia da informação o planejamento do alcance dos serviços, a utilização correta dos equipamentos, o gerenciamento de acesso e a segurança das informações.

Na Unidade 1, serão estudados os fatos históricos que levaram à necessidade de nos comunicarmos mediante redes de computadores: os meios utilizados na transmissão e comunicação; as possibilidades de implementação de aplicações nas redes; os equipamentos e a sua função. Por meios desses aspectos básicos, você poderá desenvolver redes locais de pequeno porte.

Na Unidade 2, será possível compreender a relevância do modelo de referência OSI que possibilitou a evolução e a organização das redes; identificar e classificar os serviços de rede, a hierarquia dos protocolos e como os protocolos TCP/IP são de vital importância para que ocorra a comunicação entre as redes. Com isso, será possível conhecer e configurar alguns serviços essenciais às redes de computadores.

Na Unidade 3, com a evolução dos seus conhecimentos, será possível: detalhar as classes de endereço IP e efetuar o cálculo de sub-rede; identificar as características das redes ethernet; refletir quão importante é o protocolo de comunicação IPv6 para evolução dos serviços e aplicações nas redes; e conhecer quais são as dificuldades no período de coexistência e interoperabilidade. Tais entendimentos possibilitam o cálculo e a implementação de redes divididas por faixas de endereçamento IP.

Na Unidade 4, será possível: entender os aspectos gerenciais relacionados à administração e ao gerenciamento das estruturas e

dos serviços de redes; compreender como identificar os elementos que podem degradar os serviços; saber como as regras podem garantir a QoS (Qualidade de Serviço). Com esses conteúdos, é possível desenvolver uma visão gerencial nas redes de computadores.

Caro aluno, as redes de computadores (4G, wi-fi ou cabeadas) possibilitam acessar diversos serviços necessários à população. Você, como futuro profissional de tecnologia da informação e comunicação, precisa se inteirar sobre o assunto. Vamos estudar redes de computadores?

Princípios de comunicação de dados e teleprocessamento

Convite ao estudo

As redes de computadores estão presentes na maioria dos serviços que consumimos diariamente, tanto ao passar o cartão para efetuar um pagamento, assistir a um filme por serviço *on demand* (sob demanda), quanto ao pedir comida por um aplicativo no dispositivo móvel.

Com o aumento dos serviços providos por rede, a maior oferta e disponibilidade dos provedores de internet e a popularização dos dispositivos móveis, é necessário, para a garantia e a continuidade dos serviços, que haja crescimento na formação de profissionais de tecnologia da informação que possuam conhecimentos apropriados sobre redes de computadores.

Os estudos e conhecimentos adquiridos em redes de computadores permitirão que você administre, organize e gerencie uma rede de computadores, proporcionando segurança e qualidade de serviço para que a empresa possa exercer as suas atividades.

Nas seções de aprendizagem ao longo deste livro, você terá oportunidade de compreender:

- Os aspectos históricos, os meios de transmissão, os tipos de sinais e modos de operação utilizados nas redes de telecomunicações.
- Os aspectos básicos das redes de computadores, os mecanismos envolvidos nas redes de difusão e ponto a ponto e os hardwares que podem prover a troca de mensagens.

- Os equipamentos (roteador, bridges, switch e repetidor) utilizados nas infraestruturas, as topologias, os tipos de rede segundo o nível de abrangência e as redes sem fio.

Para o entendimento das questões aqui tratadas, baseie-se no seguinte contexto:

Uma empresa que desenvolve jogos para smartphones e computadores, cuja matriz está localizada em São Paulo. São vários os jogos de sucesso desenvolvidos pela companhia e essa fama na qualidade dos seus produtos fez com que a escolas solicitassem o desenvolvimento de jogos educacionais.

A sua equipe, portanto, deve estar bem preparada para esse desafio. Vamos, então, estruturar as redes da empresa?

Seção 1.1

Introdução à comunicação de dados e ao teleprocessamento

Diálogo aberto

Os aspectos básicos e históricos no tocante à comunicação de dados, os meios e os métodos de transmissão permitirão que você compreenda quais são os serviços necessários para prover a comunicação entre as redes e como tomar uma decisão ao contratá-los. Isso será alicerce de seu conhecimento para o entendimento da evolução e das necessidades de desenvolvimento de serviços de redes de computadores.

Para suprir essa nova demanda, a empresa deseja abrir uma filial na área central da cidade de Campinas. Após algumas reuniões, a sua equipe foi indicada pelo diretor de TI para implementação, estruturação e gerenciamento da nova rede, graças às competências e habilidades demonstradas em outros projetos anteriores.

O projeto visa à implementação de uma infraestrutura de redes para a empresa R, na cidade de Campinas (área central). Para que se atendam às necessidades iniciais, algumas especificações técnicas devem ser cumpridas, como:

- Disponibilidade de serviços: SLA (Service Level Agreement – Acordo de Nível de Serviço), ou seja, o contrato com as especificações dos serviços contratados (mínimo de 95% de disponibilidade. Taxa de upload e download de 30MB).
- Valor dos pacotes de serviço.
- Link dedicado para comunicar a matriz e a filial, com fibra óptica e velocidade de 1 GB.

Para isso, você deverá fazer uma pesquisa de mercado com os planos comerciais disponíveis nas operadoras de Telecom.

A sua pesquisa deve ser apresentada para a diretoria da empresa, em formato de relatório, com as informações de pelo menos duas empresas e a justificativa do pacote recomendado pela sua equipe.

Não pode faltar

Com o crescente acesso à internet, o desenvolvimento de novos serviços de streaming (vídeo, música, filmes e jogos on-line via internet) e a popularização dos dispositivos móveis, a demanda por profissionais com conhecimento técnico para estruturação de servidores, cabeamento estruturado, configuração de equipamentos, planejamento para implementação e administração das redes cresce proporcionalmente ao consumo de seus serviços.

Nesse sentido, você já se perguntou como tudo isso começou?

O início – 1961 a 1972

Segundo Kurose (2006), os primeiros estudos relacionados a redes de computadores ocorreram no início da década de 1960. As pesquisas foram realizadas por diferentes grupos, sendo eles:

- Leonardo Kleinrock (1961 a 1964), por meio de seus estudos de doutorado no MIT, desenvolveu uma técnica de comutação de pacotes em rajadas.
- Paul Baran (1964) deu continuidade aos estudos de Kleinrock e efetuou a transmissão segura de voz em redes militares.
- Em 1967, surge a Arpanet por meio dos estudos desenvolvidos no MIT.
- Em 1969, na Universidade da Califórnia em Los Angeles (UCLA), foi instalada a primeira rede com a capacidade de transmissão de mensagens por meio de interfaces.
- Em 1972, a Arpanet possuía 15 nodos ("nodos" é o termo usado para designar nós de redes) e havia desenvolvido o primeiro protocolo de comunicação em rede, chamado NCP (Network Control Protocol).

Os primeiros estudos e desenvolvimentos ocorridos foram posteriores ao período pós-Segunda Guerra Mundial. Esses fatos históricos acabaram por beneficiar a ciência da computação, pois havia um interesse dos dois eixos envolvidos nos conflitos para a interceptação e decodificação dos códigos.

Surgimento de mais redes – 1972 a 1980

Uma década após o surgimento das primeiras técnicas aplicadas em de redes de computadores, os pesquisadores ao redor do mundo

tomaram conhecimento delas nos congressos e nas conferências que discutiam comunicação. Segundo Kurose (2006), em meados dos anos 1970, surgiram novos estudos e novas experiências das redes:

- ALOHAnet, uma rede que ligava as universidades existentes nas ilhas do Havaí, onde se utilizavam micro-ondas para prover a comunicação de dados.
- Cyclades, rede francesa que utilizava comutação de pacotes desenvolvida por Louis Pouzin.
- Rede SNA pertencente à IBM, com um trabalho próximo ao que era realizado na Arpanet.

Ainda ao final dos anos 1970, o interesse militar americano na comunicação via rede favorecia as pesquisas, pois a Darpa (*Defense Advance Research Projects Agency* – Agência de Projetos de Pesquisa Avançada de Defesa) patrocinava diversos estudos.

Nessa época, foram projetadas as primeiras versões do protocolo TCP, IP e UDP, essenciais na estruturação dos serviços de redes como conhecemos hoje.

Aumento do número de redes – 1980 a 1990

Além dos interesses militares estratégicos, o mercado vislumbrava uma potencial forma de alavancar milhares de dólares. Com isso, a iniciativa privada "entrava de cabeça" no promissor mercado de comunicação de dados, patrocinando alguns estudos e desenvolvimentos.

Kurose (2006) descreve que, ao final da década de 1980, as universidades formaram uma confederação de redes com aproximadamente cem mil dispositivos. Grande parte disso se deu no dia 1º de janeiro de 1983, quando o protocolo TCP/IP foi adotado oficialmente. Além disso, surge o sistema de controle de nomes de domínios (DNS), que possibilitou a associação de um número IP a um nome de um domínio.

Na década de 1980, o exemplo mais emblemático dos interesses comerciais e da crescente evolução dos serviços de comunicação de dados foi o projeto Minitel, desenvolvido na França. O governo francês disponibilizou para 20% da população três tipos de serviços digitais: acesso à lista telefônica, navegação por sites particulares e a utilização de *home banking* (serviços bancários).

Período evolutivo da internet – Década de 1990

Ao final da década de 1980, diversas tecnologias haviam sido desenvolvidas, porém a maior contribuição, segundo Kurose (2006), surgiu na década de 1990. A principal delas foi a *World Wide Web*, inventada no CERN (*European Center for Nuclear Physica* – Centro Europeu para Física Nuclear). Com isso, ocorreu a evolução do hipertexto para desenvolvimento de websites e dos navegadores (Netscape e Internet Explorer).

Na segunda metade dos anos 1990, tanto as empresas privadas quanto as pesquisas por meios acadêmicos fizeram com que surgissem os seguintes serviços:

- E-mail, com a possibilidade de anexar arquivos.
- *E-commerce* com a navegação web.
- Mensagens instantâneas; na época, o ICQ.
- Compartilhamento de arquivos para MP3 do tipo P2P, na época o Napster.

Figura 1.1 | Chat ICQ

Fonte: <https://goo.gl/XNVybH>. Acesso em: 3 jul. 2017.

Os altos lucros alcançados por empresas como Microsoft, Cisco, AOL, e-Bay e Amazon fizeram com que a velocidade de transmissão, novos equipamentos e métodos de acesso à internet fossem os novos alvos de pesquisas, patrocinadas para o aumento na qualidade e disponibilidade dos seus serviços.

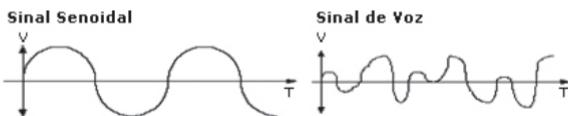
Atualmente

Na última década houve uma evolução das tecnologias desenvolvidas para a comunicação, que possibilitou a disponibilização

de serviços como: vídeo *on demand*, VoIP, jogos on-line, *streaming* de músicas, entre outros. Além disso, objetos utilizados no nosso cotidiano passaram a se conectar na rede mundial, tais como os carros, celulares, televisores, entre diversos outros dispositivos.

Repare que o desenvolvimento dos protocolos acaba por criar uma dependência funcional entre eles. Isso ocorre porque de nada adiantaria o desenvolvimento do protocolo HTTP se não houvesse o DNS para poder resolver o nome dos sites onde os hipertextos estão hospedados. E jamais um servidor, independentemente dos serviços disponibilizados, conseguiria ser atingido se não houvesse os protocolos TCP/IP. Por isso, o funcionamento de um serviço depende da sincronia de diversos protocolos nas redes atuais.

Caro aluno, para evoluirmos um pouco mais, é necessário compreender os tipos de sinais utilizados na comunicação. Vamos observar como isso está presente no nosso dia a dia. Alguns canais de televisão possuem duas opções de acesso, por sinais analógico e/ou digital, contexto em que se evidencia a evolução tecnológica do sinal digital (som e imagem).

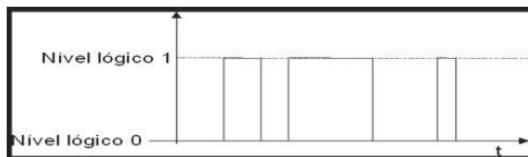
Em redes de computadores, esses dois sinais também estão presentes nos tipos de transmissão e determinam a qualidade do serviço.

Sinal analógico

Segundo Tanenbaum (1997), os sinais analógicos são ondas eletromagnéticas que assumem infinitos valores ao longo do tempo. Este sinal é representado por uma onda senoidal com as seguintes características:

- Amplitude: representa intensidade mais alta dos sinais elétricos (volts).
- Frequência: medida em hertz, define a quantidade de ciclos em um intervalo de tempo.
- Fase: define o formato da onda senoidal e pode ser medida em graus ou radianos.

Para uma melhor compreensão do sinal analógico, observe o sinal produzido pela voz humana na Figura 1.2 a seguir:

Figura 1.2 | Exemplo de sinal analógico

Fonte: <https://goo.gl/SqpmUa>. Acesso em: 3 jul. 2017.

Sinal digital

Em contrapartida, o sinal digital é representado por 0 s e 1 s, ou seja, de forma binária. A representação dos seus valores é dada como discreta ao longo do tempo e amplitude. Com isso, é possível diminuir a taxa de oscilação, fenômeno este responsável pelo aumento da qualidade de serviço. Quando ocorre uma transmissão de dados, há um processo de codificação (digitalização) desse sinal. Com isso:

- Os sinais digitais não sofrem degradação dos serviços por interferência ou ruídos.
- Pode-se transmitir maior quantidade de informações.

Observe a Figura 1.3 a seguir com as características do sinal digital.

Figura 1.3 | Exemplo de sinal digital

Fonte: <https://goo.gl/Qg4m5V>. Acesso em: 3 jul. 2017.

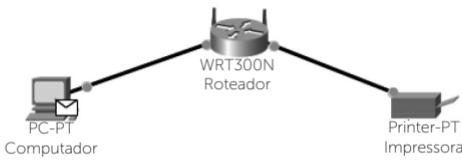
Exemplificando

Para compreender o termo "discreto ao longo do tempo", imagine que na transmissão de televisão um canal utilize sinais analógicos, com as seguintes variações:

(0.032 – 0.333 – 0.998 – 1.044 – 0.265)

No sinal digital, como os valores assumem características discretas, utilizando as mesmas medições do exemplo de sinais analógicos, teríamos que:

(0 – 0 – 1 – 1 – 0)

Ou seja, valores binários.

Esses sinais, em uma transmissão feita por uma internet cabeada (oferecida pelas operadoras), em que se pretende acessar um site a partir de um dispositivo, ocorrem da seguinte forma:

1. Os modems fornecidos pelas operadoras fazem a adequação do sinal digital com o meio disponibilizado pela operadora.

2. O modem recebe os sinais emitidos pelo computador (entende-se notebooks, tablets e smartphones) e coloca no meio de transmissão fornecido pela operadora (processo conhecido como modulação).

3. Ao chegar ao destino, é efetuado o processo inverso.

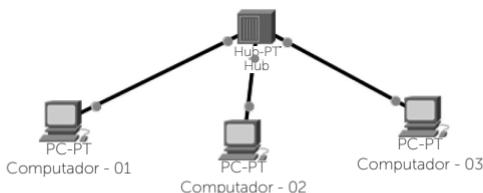
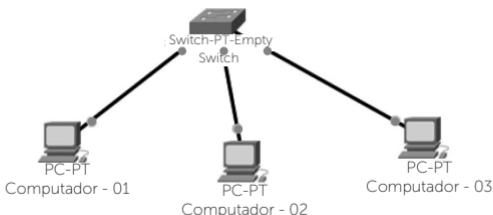
Os modos de transmissão dos sinais nas redes de comunicação de dados podem variar conforme o sentido pelo qual ocorrem as trocas de mensagens, o número de bits enviados simultaneamente e a sincronização entre computador e servidor. Basicamente, Kurose (2006) define três categorias:

Simplex: caracteriza-se pela comunicação ser em sentido único, em que um emite a mensagem e o outro a recebe. Observe a Figura 1.4 a seguir:

Figura 1.4 | Comunicação simplex

Fonte: elaborada pelo autor.

Figura 1.5 | Comunicação half-duplex

Fonte: elaborada pelo autor.

Hub é um equipamento utilizado em algumas redes para comunicar os computadores, o qual tem a capacidade de emitir e receber mensagens, porém não consegue fazer os dois processamentos de forma simultânea.

Full-duplex: caracteriza-se pela capacidade de transmitir e receber as mensagens de forma simultânea. Observe a Figura 1.6 a seguir:

Figura 1.6 | Comunicação full-duplex

Fonte: elaborada pelo autor.

O *switch* é um equipamento para interligar redes e tem a capacidade de emitir e receber mensagens simultaneamente.

Reflita

Existem diversos equipamentos no dia a dia das pessoas que utilizam os três modos de transmissão: simplex, half-duplex e full-duplex. São modos utilizados para prover a comunicação, encontrados nas casas, no trabalho e no convívio das pessoas. De que forma podem ser identificados os três modos de transmissão em dispositivos utilizados diariamente?

Meios de transmissão

Tanenbaum (1997) define que, para que os sinais possam ser transmitidos, existem dois tipos de meios de transmissão:

- Guiado:

- Par-trançado: nesta modalidade os fios são enrolados de forma helicoidal, pela qual ocorre menos interferência, uma vez que as ondas formadas em volta dos fios se cancelam. Esses fios suportam sinais analógicos e digitais nas suas transmissões e são divididos em CAT 5, 5e, 6 e 7, que se diferenciam pela largura de banda suportada ou pela presença ou não de blindagem.

- Cabo coaxial: o cabo tem um núcleo de cobre, envolto por uma camada plástica isolante, que, por sua vez, é circundada por uma malha externa. Possibilita ligar redes com distância maiores, maior velocidade que o par trançado e recebe menos ruídos. São dois tipos utilizados na comunicação de dados, coaxial 10Base2 para taxas de transmissão de 10 Mbps e segmentos de até 185 m e o cabo 10Base5, para redes de banda larga e alcance de até 500 m.

- Fibra óptica: o cabo de fibra é constituído por um núcleo e uma casca de sílica em sua volta. A luz é injetada por *leds* onde os dados são transmitidos. Ao receber as informações, o sinal óptico é transformado em sinal elétrico. Nesse tipo de transmissão, é possível alcançar velocidade de até 10 terabytes por segundo.

Pesquise mais

A capacidade de transmissão e a qualidade alcançada com a fibra óptica faz com que as empresas invistam em melhoria das redes. Um grupo de pesquisadores brasileiros do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD) conseguiu atingir um recorde na distância transmitida e na taxa de transmissão.

O artigo intitulado *Informação Muito Mais Rápida*, de Batista (2016), descreve a condução dos experimentos a qualidade que pode ser atingida com a descoberta.

Disponível em: <http://revistapesquisa.fapesp.br/wp-content/uploads/2016/08/070-071_Fot%C3%B4nica_246.pdf?4aecbb>. Acesso em: 2 mar. 2017.

• Não guiado:

- Rádio: o sinal do rádio é feito por torres de transmissão até o ponto de instalação das antenas receptoras. Apesar das distâncias alcançadas, o sinal recebe atenuação de vários obstáculos, como as construções, as árvores, além das interferências climáticas e, com isso, há perda na qualidade e às vezes até falha no sinal.

- Micro-ondas: neste tipo de transmissão, as ondas viajam em linha reta entre o emissor e o receptor; portanto, para fazer a ligação entre duas redes, faz-se necessário que haja visada entre as antenas. Pode-se atingir uma distância de até 80 km com uma antena elevada 100 m do solo, em uma geografia plana.

- Satélites: neste meio de transmissão, os sinais são enviados para os objetos que ficam estacionados acima da atmosfera terrestre, conhecidos como geoestacionários. São divididos em LEO (*Low Earth Orbit* – órbita terrestre baixa), MEO (*Medium Earth Orbit* – órbita terrestre média) e HEO (*Hight Earth Orbit* – órbita terrestre alta). Tais transmissões podem sofrer atrasos graças à distância entre emissor e receptor, além das interferências climáticas.

Os meios escolhidos para a transmissão podem variar conforme disponibilidade de infraestrutura, geografia, distância entre os pontos, viabilidade financeira, entre outros propósitos.

Sem medo de errar

Uma empresa que produz jogos para computadores e smartphones. A fim de atender à demanda das escolas de Campinas de que se desenvolvam jogos educacionais, os diretores da empresa resolveram abrir uma filial nessa cidade.

A sua equipe, então, foi selecionada para estruturar a rede da empresa – Campinas. Para atender às questões iniciais, deve ser desenvolvido um relatório com uma pesquisa de mercado realizada em duas empresas de telecomunicações, que atenda às seguintes especificações técnicas:

- Link de internet: SLA mínima de 95%, taxa de upload e download de 20 Mb.
- Valor dos pacotes de serviço.
- Link dedicado para comunicar a matriz e a filial, com fibra óptica e velocidade de 100 Mb.

RELATÓRIO DE PESQUISA DE MERCADO

Empresa A (link dedicado)

1 gb (full-duplex).

SLA 98%.

Fibra e rádio com redundância.

Instalação de equipamentos por comodato R$ 280,00.

Link dedicado 100 Mb R$ 5.000,00.

Empresa B (link dedicado)

1GB (full-duplex).

SLA 99%.

Fibra sem redundância.

Instalação de equipamentos por comodato R$ 0,00.

Link dedicado 100 Mb R$ 4.750,00.

Empresa A (internet)

20MB (full-duplex).

SLA 95%.

Fibra sem redundância.

Instalação de equipamentos por comodato R$ 0,00.

Link de internet 20 Mb R$ 250,00.

Empresa C (internet)

20MB (full-duplex).

SLA 97%.

Fibra sem redundância.

Instalação de equipamentos por comodato R$ 0,00.

Link de Internet 20 Mb R$ 210,00.

Conclui-se que:

Link de internet: a empresa C apresenta maior disponibilidade de entrega de serviços, 2% a mais que a empresa A, além de representar uma economia anual de aproximadamente R$ 500,00.

Link dedicado: a empresa A possui SLA 1% menor que a empresa B, porém a redundância oferecida pela empresa pode oferecer SLA maior que a especificada. O custo é mais elevado, porém a qualidade dos seus serviços pode garantir as necessidades técnicas da empresa.

Avançando na prática

Meios de transmissão entre dois prédios

Descrição da situação-problema

O supermercado Com_2as, localizado na cidade de São Paulo, possui o depósito na Rua José Castro de Freitas Filho (D) e a sua

loja na Rua Gotaru Suzuki (S), conforme demonstra a Figura 1.7 a seguir.

Figura 1.7 | Localização do supermercado

Fonte: Google Maps.

A distância aproximada dos dois pontos é de 200 m. Sabendo que os meios de transmissão possuem restrições quanto à distância, a fim de evitar a degradação dos serviços, faz-se necessário comunicar o depósito com a loja, sem que ocorra perda na qualidade da conexão.

Resolução da situação-problema

São três opções possíveis para efetuar a comunicação entre o depósito e a loja, sendo elas:

- Cabo coaxial: o cabo do tipo 10Base5 possibilita um alcance de até 500 m de distância entre dois pontos; ponto positivo: o custo; ponto negativo: a instalação em áreas em que o cabo fique exposto a intempéries climáticas.
- Fibra óptica: o cabo pode alcançar longas distâncias sem que ocorra a degradação dos serviços; ponto positivo: a velocidade da comunicação; ponto negativo: o custo do metro do cabo.
- Rádio: a comunicação sem fio possibilita comunicar pontos distantes sem a necessidade de instalação de cabeamento; ponto positivo: baixo custo; ponto negativo: suscetível às condições climáticas.

Embora o valor da fibra óptica seja maior que as outras opções, esta se mostra mais adequada, pois pode garantir qualidade na

comunicação entre os dois prédios. Em razão de a distância não ser muito longa, o custo-benefício quanto à baixa manutenção da fibra óptica justifica o investimento.

Faça valer a pena

1. Desde o início da década de 1960, as redes de comunicação despertaram interesses acadêmicos, militares e, alguns anos depois, industriais também. Os interesses desses diferentes grupos podiam ser diferentes, porém as contribuições fizeram com que, em três décadas, houvesse uma surpreendente evolução dos seus serviços.
Com base nesse contexto histórico da evolução das redes de comunicação, observe as afirmativas a seguir:
I. No início das redes de comunicação, o período pós-guerra favoreceu a evolução dos serviços e protocolos, pois havia interesse político-militar no desenvolvimento da promissora ferramenta.
II. A ALOHAnet foi uma rede que conseguiu ligar dois continentes, pois utilizava como meio de transmissão o sinal de micro-ondas, que possibilita interligar longas distâncias.
III. A década de 1990 foi marcada pelo desenvolvimento da *World Wide Web*, o que possibilitou posteriormente o surgimento dos serviços de e-mail, *e-commerce* e P2P.
Assinale a alternativa CORRETA:

a) Somente a afirmativa I é verdadeira.
b) Somente as afirmativas I e III são verdadeiras.
c) Somente a afirmativa II é verdadeira.
d) Somente as afirmativas I e II são verdadeiras.
e) As afirmativas I, II e III são verdadeiras.

2. Os tipos de sinais utilizados na comunicação de dados podem ser determinantes na QoS (*Quality of Services* – qualidade de serviço) das aplicações que utilizamos diariamente, tanto na transmissão de canais de televisão quanto nos serviços de internet como *streaming* de filmes, áudio ou jogos on-line. Os sinais utilizados nas comunicações são do tipo analógico e digital.
Quanto às características e funções dos sinais utilizados na comunicação de dados, indique (V) nas afirmativas verdadeiras ou (F) nas falsas:
( ) Os sinais analógicos são ondas eletromagnéticas que possuem frequência, fase e amplitude.
( ) A amplitude afere a intensidade mais alta dos sinais elétricos em Hertz.

( ) Os sinais gerados pela tecnologia digital variam entre 0 e 1. São considerados discretos no tempo e amplitude em razão de sua taxa de variação.
( ) A onda gerada pelo sinal analógico tem o formato senoidal.
( ) Os serviços gerados pelo sinal digital apresentam uma queda de qualidade ante o sinal analógico.

Assinale a alternativa com a sequência correta de indicações, de cima para baixo:
a) F – V – F – F – V.
b) V – F – V – F – V.
c) F – V – F – V – F.
d) V – F – V – V – F.
e) F – F – F – V – V.

3. As tecnologias desenvolvidas para comunicar equipamentos e redes distribuídas geograficamente proporcionam que as barreiras e distâncias possam ser vencidas, a fim de comunicar empresas e pessoas.
As formas de comunicação utilizadas podem variar em custo, alcance, velocidade de transmissão e forma de transmissão (guiada e não guiada).
Observe os dispositivos a seguir e indique (G) para transmissões guiadas e (NG) para transmissões não guiadas.
(   ) Coaxial.
(   ) Rádio.
(   ) Micro-ondas.
(   ) Fibra óptica.
(   ) Par trançado.

Assinale a alternativa que apresente a sequência CORRETA de indicações, de cima para baixo:

a) G – NG – NG – G – G.
b) NG – NG – G – G – NG.
c) NG – G – NG – G – NG.
d) G – G – G – NG – G.
e) G – NG – NG – NG – G.

Seção 1.2

Introdução a redes de computadores

Diálogo aberto

Na seção passada, você pôde compreender:

- Os fatos históricos que ajudaram na evolução das redes de comunicação.
- Os tipos de sinais utilizados para prover a troca de mensagens.
- O formato das operações realizadas em telecomunicações.

Você conheceu também os meios de transmissão que são utilizados nas estruturas físicas.

Neste momento, aluno, você compreenderá:

- Os aspectos técnicos das redes de computadores.
- As aplicações possíveis nas infraestruturas disponíveis.
- O funcionamento e os mecanismos envolvidos nas redes de difusão e ponto a ponto.
- A forma como os hardwares básicos auxiliam para que a comunicação de dados ocorra.

Tais conhecimentos vão auxiliá-lo a planejar e estruturar uma rede, utilizando alguns equipamentos simples para prover a comunicação entre os dispositivos de uma rede.

Como já dito, é uma empresa que desenvolve jogos para computadores e smartphones, cuja matriz se localiza na cidade de São Paulo. Graças a um contrato com as escolas do município de Campinas, uma filial foi instalada na cidade. O diretor de TI, no entanto, está apreensivo, pois os desenvolvedores só podem dar início às suas atividades quando o novo endereço possuir uma infraestrutura de rede mínima.

Para isso, foi solicitado que a matriz disponibilizasse alguns equipamentos como desktops, impressoras, roteador e hub, para que fossem instalados na planta baixa a seguir:

Figura 1.8 | Planta baixa – Filial Campinas

Fonte: <https://goo.gl/UOrhHe>.

Os equipamentos devem ser instalados da seguinte forma:

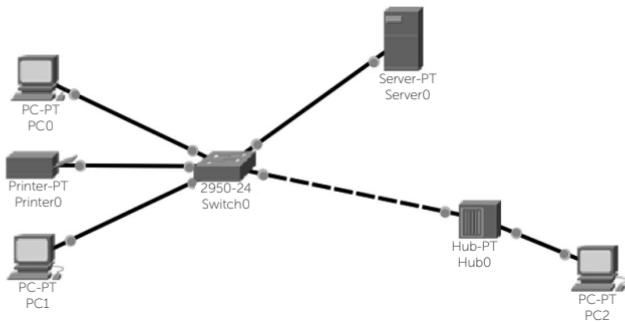
- Recepção **(R)**: 1 computador.
- Sala do Gerente de Projetos **(G)**: 1 computador, 1 impressora.
- Sala de desenvolvimento **(D)**: 4 computadores; 1 impressora, 1 hub.
- Sala de reunião **(R)**: 1 roteador, 1 hub.

Caro estudante, com base na infraestrutura mencionada anteriormente, você deverá efetuar as configurações e o desenvolvimento da infraestrutura das redes, no software de simulação de redes de computadores Packet Tracer. Para isso, faça download da versão apropriada ao seu sistema operacional, disponível em: <http://labcisco.blogspot.com.br/p/laboratorios.html>. Acesso em: 12 mar. 2017.

O Packet Tracer é um software que permite simular uma estrutura de rede, com diversos equipamentos como: desktops, notebooks, roteador, *switch*, hub, servidores e seus serviços (e-mail, FTP, DNS, DHCP, HTTP, entre outros).

De que forma a sua equipe pode utilizar os equipamentos de hardware de rede básicos para que a rede possam funcionar dentro do padrão de qualidade esperado?

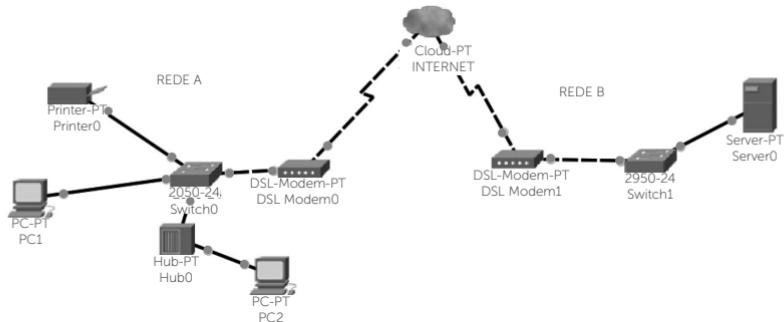
Pronto para esse novo desafio? Vamos lá!

Não pode faltar

É notório como houve uma evolução significativa nas aplicações que utilizamos por meio da internet, e a cada dia criamos uma dependência desses serviços pela comodidade que podem proporcionar. Todos esses elementos estão presentes nos aplicativos de celular, nos meios de pagamentos eletrônicos (cartão de debito e crédito, internet banking), entre diversos outros serviços que utilizamos no nosso cotidiano.

Mas, por trás de todos esses serviços consumidos diariamente, existe uma infraestrutura que deve ser planejada e administrada para garantir a continuidade das aplicações e a qualidade dos seus serviços.

Segundo Tanenbaum (1997), as empresas têm um número significativo de computadores, dispositivos e sistemas. O compartilhamento desses recursos é um dos primeiros desafios do administrador de redes, pois elas devem permitir que os usuários possam utilizar os mesmos dispositivos como impressoras, repositório de arquivos e as funcionalidades que cada sistema possui.

Nas primeiras redes era possível compartilhar os arquivos e dispositivos das redes dentro de uma mesma organização, conforme pode ser observado na figura a seguir:

Figura 1.9 | Compartilhamento em rede local

Fonte: elaborada pelo autor.

Na rede de exemplo, pode-se perceber que os dispositivos PC0, PC1, Printer0 (impressora), Server0 e Hub0 estão diretamente ligados por meio do Switch0, já o PC2 está indiretamente ligado aos demais dispositivos pelo Hub. Os computadores dessa rede podem

compartilhar a impressora e os arquivos por meio do servidor. Porém, repare que essa rede não possibilita acesso externo.

Com o advento da internet, as aplicações e os compartilhamentos possíveis não estavam mais presos aos dispositivos da rede local, conforme demonstrado na figura a seguir:

Figura 1.10 | Compartilhamento em redes distintas

Fonte: elaborada pelo autor.

Caro aluno, observe que, na Rede A, estão localizados os computadores e as impressoras; na Rede B, imagine que por uma questão de segurança o servidor está localizado em outra cidade. Por meio das técnicas de endereçamento é possível acessar serviços e dispositivos em qualquer lugar com internet.

Para conceituar os exemplos anteriores, Forouzan (2006) define que em uma rede privada os recursos e sistemas compartilhados ficam restritos à organização e podem estar estruturados de duas formas:

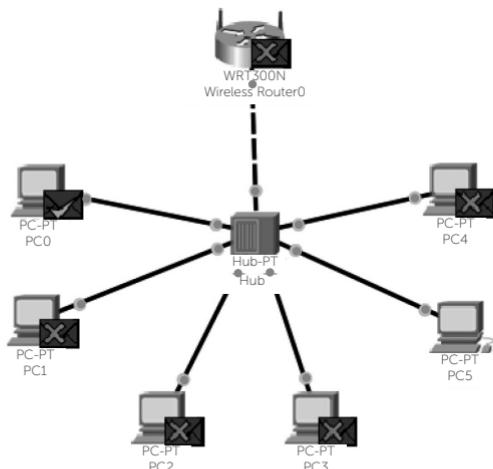
- Intranet: compreende uma rede privada que utiliza em sua estrutura física e lógica o modelo de internet. Porém, os serviços de rede como servidores de arquivos e impressão, servidor web e as aplicações são de uso interno.
- Extranet: conhecida popularmente como internet, tem como diferença o fato de que os recursos só podem ser acessados com autorização de um administrador da rede de uma companhia.

Segundo Forouzan (2006), o conjunto dos vários dispositivos e links que possibilitam conectar redes geograficamente distribuídas, ou mesmo as redes locais, deve atender aos seguintes critérios:

- Desempenho: normalmente é medido pelo tempo que uma mensagem leva para ir de um dispositivo a outro. Algumas métricas, como vazão, atraso ou perda de pacotes, são indicadores de degradação dos serviços (Na Unidade 4 isso será estudado com maiores detalhes).
- Confiabilidade: mede a frequência com que as falhas de desempenho ocorrem e o tempo durante o qual a rede leva para se recuperar. O gerenciamento da confiabilidade pode ajudar a garantir a QoS (*Quality of Services* – Qualidade dos Serviços).
- Segurança: garantir a não ocorrência de incidentes de acesso não autorizado, a proteção quanto aos danos causados e a implementação das políticas de segurança.

Para medir o desempenho de taxa de upload e download, alguns sites fornecem uma ferramenta para auxiliar os profissionais que trabalham com infraestrutura de redes a diagnosticar problemas como atraso na entrega das mensagens. Com isso é possível saber se o pacote contratado atende às necessidades da empresa, conforme exemplificado a seguir:

- Taxa de Download: 10,53 Mbps
- Taxa de Upload: 1, 04 Mbps
- Latência: 18,26 ms
- Perda de Pacotes: 0%
- Jitter: Nulo

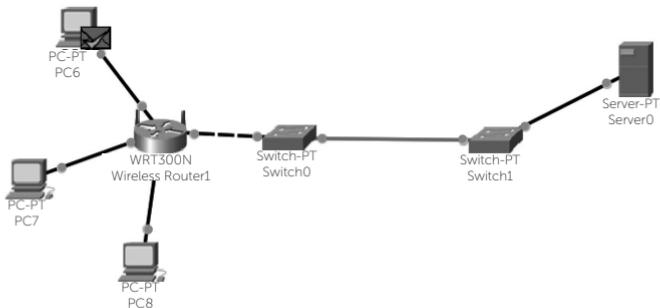
Os testes foram efetuados no site: <http://www.brasilbandalarga.com.br/speedtest>. Acesso em: 6 mar. 2017.

Caro aluno, todas as características de infraestruturas e aplicações possíveis que as redes de computadores podem proporcionar demonstram a importância econômica que podem representar para uma população a correta administração e o correto gerenciamento dos serviços providos pelas redes.

Para prover a comunicação entre dois pontos distintos, independentemente de a rede ser interna ou externa, Tanenbaum (1997) define que existem dois tipos de tecnologias que são utilizados: os links de difusão e os links ponto a ponto.

Redes de Difusão:

Nas redes de difusão, existe apenas um canal de comunicação em que todas as máquinas compartilham esse meio. A mensagem é enviada por meio de um pacote, que contém o endereço do destinatário. Esse pacote é enviado a todos os dispositivos da rede, e cada um dos computadores, ao receber a mensagem, verifica o endereço. Se for destinado à máquina, o pacote é processado, senão a mensagem é descartada. Essa técnica é demonstrada na figura a seguir:

Figura 1.11 | Exemplo de Rede de Difusão

Fonte: elaborada pelo autor.

Observe que na rede acima foi enviada uma mensagem do PC5 para o PC0. Ao receber a mensagem, cada computador verifica o endereço do destinatário: se for negado, é colocado um "X" em vermelho; o PC0, por sua vez, confirma o recebimento com um "V" na cor verde.

Kurose (2006) exemplifica que as rádios FM utilizam redes de difusão, pois as estações de transmissão enviam os sinais para os rádios receptores que se encontram nas residências e nos veículos.

Redes Ponto a Ponto:

Neste tipo de rede, os pacotes percorrem por diversos dispositivos intermediários até atingir o destino correto. Observe a figura a seguir:

Figura 1.12 | Exemplo de Rede Ponto a Ponto

Fonte: elaborada pelo autor.

No exemplo anterior, a rede à esquerda representa um escritório localizado em uma cidade qualquer; a rede à direita, por sua vez, é um servidor localizado em outro estado. O PC6 faz ao Servidor (Server0) uma solicitação para acessar um site, e a mensagem com a resposta que permite abrir o site no navegador é enviada somente ao dispositivo solicitante. Dessa forma, constrói-se uma rede ponto a ponto, em que a comunicação é feita entre transmissor e emissor, independentemente de quantos caminhos e nodos o pacote tenha que passar até atingir o destino correto.

Pesquise mais

Toda vez que uma mensagem é enviada para um dispositivo que não se encontra no mesmo local, ela pode percorrer vários caminhos distintos. Para entender esse conceito, faça os seguintes passos.

1. Abra o Prompt de Comando (cmd).

2. Digite: tracert google.com.br (no Linux traceroute)

Observe que ao efetuar esse comando uma solicitação é feita ao servidor do Google, e esta mensagem passa por vários nodos que são identificados na medição.

O vídeo (disponível em: <https://www.youtube.com/watch?v=lqcp3k8DgGw>; acesso em: 15 mar. 2017) demonstra como uma mensagem "viaja" da origem ao destino nas solicitações efetuadas.

Segundo Tanenbaum (1997), as formas como as mensagens são transmitidas, em regra geral, são por:

- Redes geograficamente localizadas: a tendência é utilizar a transmissão por difusão.
- Redes de longas distâncias: normalmente se utiliza a transmissão ponto a ponto.

Em alguns projetos de redes específicos podem ocorrer exceções, a fim de atender às suas necessidades e especificidades.

Caro aluno, você deve ter percebido que, para estruturar as redes, existem alguns componentes de hardware que são básicos porém essenciais para prover a comunicação entre os dispositivos. Entre eles estão:

- **Placas de Rede:**

Comer (2007) define que correspondem a um dispositivo de E/S (entrada/saída) que se conecta por meio de cabeamento aos nodos de rede (Hub, roteador, *switch* ou brigde). O controlador de interface da rede (NIC – *Network Interface Controller*) pode estar ou não integrado à placa-mãe.

Figura 1.13 | Placa de Rede

Fonte: <https://goo.gl/UIpX8G>.

A arquitetura de seu barramento pode ser na forma PCI, PCI Express, ISA e USB, ou seja, o formato de encaixe na placa-mãe. A sua função lógica é efetuar o tratamento de endereçamentos, no envio e recebimento das mensagens.

- **Modem:**

Segundo Forouzan (2006), o modem tem a função de fazer a modulação e a demodulação das mensagens, podendo também ser

conhecido como transceptor. O Quadro 1.1 a seguir demonstra os tipos de modems disponíveis e as suas respectivas funções:

Quadro 1.1 | Modems: tipos e funções

TIPO	FUNÇÃO
Analógico	Transmissão por canal de voz
Cable Modem	Transmissão de TV a cabo
ADSL	Par de fios da linha de assinante
Canal E1, E3 e E4	Canais digitais de telecomunicações
Ópticos	Transmissão por fibras ópticas

Fonte: elaborado pelo autor.

Em sua forma analógica os dados são transmitidos pelo canal de voz; por sua vez, em sua forma digital, é feita a codificação da banda base. Este equipamento está entre os mais populares dos hardwares encontrados nas redes, conforme pode ser observado a seguir:

Figura 1.14 | Modem DSL

Fonte: <https://goo.gl/E8vlWy>.

Com a maior oferta de prestadoras de serviços de internet, o dispositivo é cada vez mais encontrado nos lares brasileiros. Atualmente, o mercado oferece modems do tipo residencial, com conexão cabeada, 4G e fibra óptica, com a possibilidade de wi-fi integrado.

- Hub:

Taenenbaum (1997) define que o Hub pode conter várias linhas de entrada que são responsáveis por distribuir conexão. Esse equipamento assume o papel de um repetidor, pois a mensagem, ao chegar, é replicada para todas as portas. Observe na figura a seguir o exemplo de um Hub:

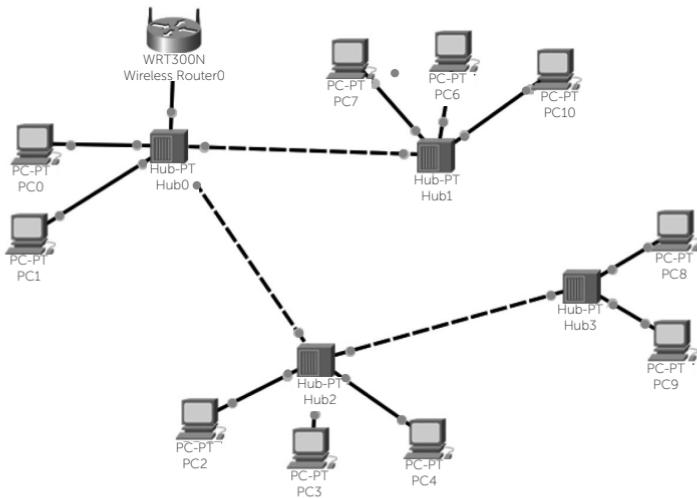



Figura 1.15 | Hub

Fonte: <https://goo.gl/fYyvHi>. Acesso em: 3 jul. 2017.

Por ter o comportamento de repetidor dentro de uma rede e por replicar uma mensagem para todos os dispositivos conectados a ele, deve-se evitar o cascateamento. Observe o exemplo da rede a seguir:

Figura 1.16 | Exemplo de cascateamento com Hub

Fonte: elaborada pelo autor

O cascateamento não necessariamente deve ser evitado com a utilização do Hub apenas, mas sim de qualquer outro dispositivo como roteador, *switch* ou bridge. Ao ser enviada uma mensagem, a cada processamento efetuado pelos dispositivos intermediários, maior será o tempo para recebimento dela pelo destinatário.

Ao utilizar o Hub, a banda disponível na rede pode ser ocupada por um número excessivo de mensagens desnecessárias em razão de o

equipamento não ler endereçamento de rede e replicar a mensagem recebida a todos os dispositivos.

Reflita

O Hub pode prover a conexão entre os dispositivos de redes, porém, graças ao excesso de mensagens que ele envia ao replicá-la para todos os dispositivos, acaba por ocupar a largura de banda e há consequente aumento do consumo de processamento dos dispositivos intermediários.

O Hub pode diminuir a QoS (Qualidade de Serviço) dos serviços providos por uma rede?

Sem medo de errar

A empresa assumiu um contrato de desenvolvimento de jogos educacionais para as escolas da cidade de Campinas. Para isso, foi locado um novo endereço com as características da planta baixa a seguir:

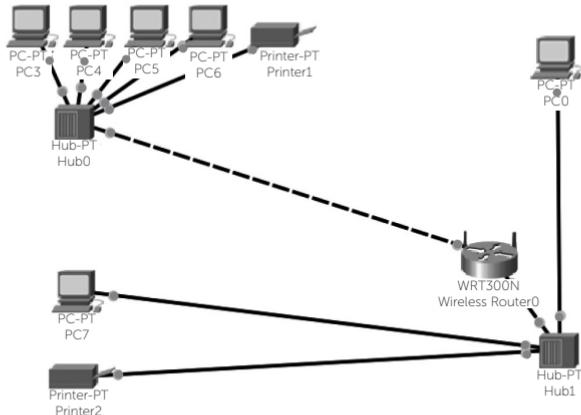
Figura 1.17 | Planta baixa – Filial Campinas

Fonte: <https://goo.gl/Fgi3OR>. Acesso em: 3 jun. 2017.

Os equipamentos devem ser instalados da seguinte forma:

- Recepção **(R)**: 1 computador.
- Sala do gerente de projetos **(G)**: 1 computador, 1 impressora.
- Sala de desenvolvimento **(D)**: 4 computadores, 1 impressora, 1 hub.
- Sala de reunião **(R)**: 1 roteador, 1 hub.

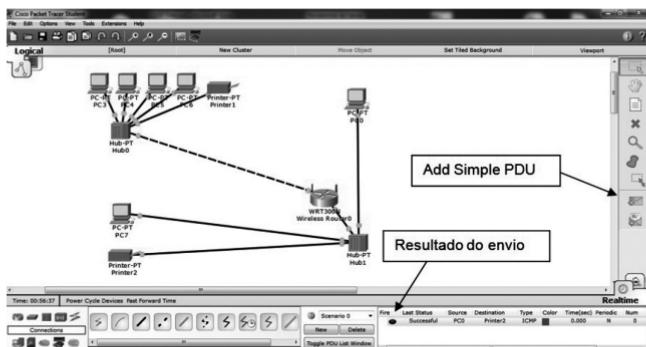
Para realizar essa atividade, você deverá utilizar o software Packet Tracer e instalar os equipamentos, conforme solicitado.

Na barra inferior esquerda estão os menus de cada um dos equipamentos. Devem ser utilizados os seguintes tipos:

- Computador: *End devices* → Primeiro dispositivo *Generic*.
- Impressora: *End devices* → Quarto dispositivo *Generic*.
- Hub: Hubs → Primeiro dispositivo *Generic*.
- Roteador → *Wireless Device* → WRT300N.
- Cabeamento para ligar computador no Hub: *Connections* → *Cooper Straight-Throught*.
- Cabeamento para ligar Hub no Roteador: *Connections* → *Cooper Cross-Over*.

Inicialmente, os equipamentos são disponibilizados nas salas; depois disso, os Hubs devem ser conectados ao roteador (cabo *cross-over*) nas seguintes interfaces:

- Porta 0 do Hub 0 na porta Ethetnet 1 do roteador.
- Porta 1 do Hub 0 na porta Ethetnet 2 do roteador.

Para conectar os demais dispositivos da rede, como computadores e impressoras, deve ser utilizada a interface de rede FastEthernet em quaisquer das portas disponíveis em um dos Hubs (cabo *Cooper Straight-Throught*), ficando da seguinte forma:

Figura 1.18 | Rede da empresa

Fonte: elaborado pelo autor.

Para que a rede funcione, um endereço deve ser configurado em cada um dos dispositivos. Para isso:

- Nos computadores: clique em cima do computador → Aba "Desktop" → Opção "Ip Configuration" → Marque a opção "DHCP".
- Nas impressoras: clique em cima da impressora → Aba "Config" → Em "Gateway/DNS", marque a opção "DHCP".

Para efetuar os testes de conectividade dos equipamentos, clique em cima do envelope disponível no menu lateral direito (*Add Simple* PDU), em seguida clique no dispositivo de origem da mensagem e um de destino. Na parte inferior do menu apresenta-se o sucesso ou a falha ao enviar, conforme pode ser observado na Figura 1.19 a seguir:

Figura 1.19 | Teste de conectividade

Fonte: elaborada pelo autor

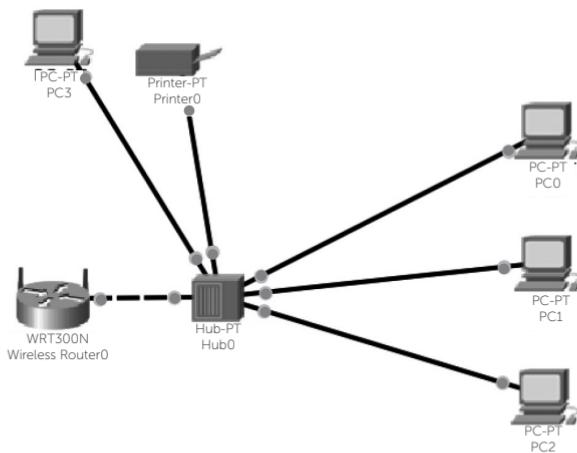
Avançando na prática

Minimercado

Descrição da situação-problema

O Jd. Nova Esperança, localizado na cidade de Esperandópolis, acabou de ter casas entregues aos moradores. No entanto, o novo bairro se encontra distante demais da área central. O sr. João adquiriu um terreno ao lado de sua residência, a fim de construir um minimercado para atender às necessidades dos moradores locais.

O estabelecimento necessita da seguinte infraestrutura: 3 computadores para os caixas; 1 computador e 1 impressora para o gerente; 1 roteador; 1 Hub.

Você foi contratado para configurar e estruturar a rede. Para isso, deve ser utilizado o software para simulação e modelagem de redes de computadores, o Packet Tracer.

Resolução da situação-problema

Para estruturar a rede do minimercado do sr. João, devem ser utilizados os seguintes equipamentos:

- **Computador**: *End devices* → Primeiro dispositivo *Generic*.
- **Impressora**: *End devices* → Quarto dispositivo *Generic*.
- **Hub**: Hubs → Primeiro dispositivo *Generic*.
- **Roteador**: Roteador → *Wireless Device* → WRT300N.
- **Cabeamento para ligar computador no Hub**: *Connections* → *Cooper Straight-Throught.*
- **Cabeamento para ligar Hub no Roteador**: *Connections* → *Cooper Cross-Over*.

Dessa forma, a rede foi simulada no Packet Tracer, como demonstrado a seguir:

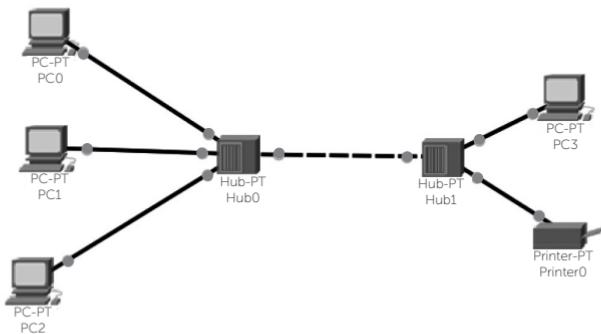
Figura 1.20 | Rede do minimercado

Fonte: elaborada pelo autor.

Como os computadores e as impressoras não possuem endereçamento, é necessário marcar a opção DHCP nos respectivos dispositivos, a fim de prover a comunicação.

Faça valer a pena

1. Uma empresa de engenharia civil desenvolve projetos para shopping. Em razão dos tamanhos dos arquivos gerados para elaborar a planta baixa, é necessário disponibilizar na rede um servidor de arquivos e um servidor de impressão, uma vez que, dessa forma, os engenheiros podem acessar outros projetos e deixar as impressões na fila do servidor.
Tal estrutura deve garantir que pessoas externas à empresa não acessem os servidores.
Assinale a alternativa que descreve o tipo de rede apropriada para atender às necessidades da empresa.
a) Extranet.
b) Internet.
c) Intranet.
d) Ethernet.
e) Fastnet.

2. Para que ocorra a troca de mensagens entre os dispositivos em uma rede de computadores, são necessários diversos hardwares envolvidos nesses processos, já que, dessa forma, é possível efetuar transmissão, encaminhamento e recepção dos sinais enviados.
Associe as colunas segundo os hardwares e os tipos possíveis:

(A) Placa de Rede	( ) ISA
(B) Modem	( ) ADSL
	( ) Canal E1, E3 e E4
	( ) PCI
	( ) Óptico

Assinale a alternativa com a sequência correta de associações, de cima para baixo:
a) A – A – B – B – A.
b) A – B – B – A – B.
c) B – A – A – A – B.
d) A – B – A – B – A.
e) B – A – A – B – A.

3. Para prover a comunicação entre dois setores de uma empresa, foram utilizados dois Hubs, conforme pode ser observado a seguir:

Fonte: elaborado pelo autora

Isso possibilitou a troca de arquivos entre os dispositivos e o compartilhamento da impressora.

Com base nas características e funcionalidades do Hub nas redes de computadores, observe as afirmativas a seguir:

I. Ao ser utilizado em uma rede, o Hub tem o comportamento de repetidor.

II. O cascateamento de Hub aumenta a quantidade de computadores possíveis e não diminui o desempenho da rede.

III. As mensagens que passam pelo Hub são replicadas para todas as portas disponíveis.

Assinale a alternativa CORRETA:

a) Apenas a afirmativa III é verdadeira.

b) Apenas as afirmativas II e III são verdadeiras.

c) Apenas a afirmativa II é verdadeira.

d) Apenas as afirmativas I e III são verdadeiras.

e) As afirmativas I, II e III são verdadeiras.

Seção 1.3

Topologias de redes

Diálogo aberto

A compreensão dos equipamentos utilizados nas redes de computadores e as suas funcionalidades e características são pontos essenciais para que os profissionais de Tecnologia da Informação possam planejar a topologia, os serviços providos e os recursos que serão compartilhados.

Além disso, a identificação das redes quanto ao nível de abrangência possibilitará efetuar o gerenciamento de redes geograficamente distribuídas, de forma eficaz.

A empresa já está instalada em seu novo endereço na cidade de Campinas, para desenvolvimento de jogos educacionais voltados aos estudantes das escolas desse município. A fim de que não ocorresse atraso no projeto, o diretor de TI solicitou que fossem instalados alguns equipamentos disponibilizados pela matriz localizada na cidade de São Paulo. Porém, no decorrer da semana, relatou-se pelos desenvolvedores e demais colaboradores lentidão no compartilhamento dos arquivos e na impressão.

Como já era previsto, esses problemas ocorreram graças ao cascateamento efetuado com os Hubs. Para solucionar esses problemas e garantir a QoS (Qualidade de Serviços), os seguintes equipamentos foram adquiridos pela Empresa:

- Sala de gerente de projetos: 1 servidor (modelo *Generic*), 1 notebook.
- Sala de desenvolvimento: 1 *switch* (modelo *Generic*), 3 notebooks.
- Notebooks conectados no wi-fi do roteador da sala de reuniões.

Dessa forma, os dois hubs da rede devem ser substituídos pelo *switch*, fazendo com que se reduza o tráfego de mensagens inúteis. Além disso, deve ser instalado um Servidor na sala do gerente de projetos, para que futuramente sejam configurados alguns serviços

de redes. Por fim, precisa ser disponibilizada conexão sem fio na recepção para os notebooks da sala de desenvolvimento e para o gerente de projetos e no roteador já instalado (anteriormente) na sala de reunião.

Para que ocorram todas essas mudanças, você deve utilizar os novos equipamentos no software de simulação de redes Cisco Packet Tracer, a fim de garantir a qualidade de conexão da rede. Para isso, modifique a rede estruturada com os Hubs e demais equipamentos para que os colaboradores da empresa possam desenvolver os jogos educacionais dentro do prazo estipulado.

Dessa forma, com a substituição dos equipamentos e a mudança da topologia, quais tipos de melhorias podem ocorrer na rede?

Ficou curioso? Vamos, então, encarar mais esse desafio.

Não pode faltar

As redes utilizadas diariamente possuem em suas infraestruturas alguns equipamentos essenciais para prover a comunicação entre os dispositivos independentemente da sua localização geográfica. Tais equipamentos e as suas respectivas configurações são imperceptíveis para o usuário final, porém o desempenho dos seus serviços pode ser sentido (positivamente ou negativamente).

Caro aluno, com base nisso, é necessário que você saiba identificar os equipamentos de hardware, as topologias (pode-se ser definido como mapa da rede) possíveis em algumas redes, o nível de abrangência das redes (PAN, LAN, MAN, WAN e SAN), a definição das redes distribuídas e sem fio.

Os equipamentos que serão discutidos nesta seção não serão detalhados ao nível de camadas do modelo de referência OSI, pois isso será feito na Seção 1 da Unidade 2

Roteador

Forouzan (2006) define que os roteadores são hardwares de redes que contêm microprocessadores, responsáveis pelo gerenciamento dos tráfegos de pacotes de dados, porém, diferentemente do Hub, ele tem a capacidade de analisar o endereçamento lógico (TCP/IP).

O roteador forma tabelas lógicas dos equipamentos disponíveis nas redes, como: roteador, *switch,* computadores, dispositivos

móveis, impressoras IP e câmeras IP. Para auxiliar nesse processo, é utilizado um mecanismo de descoberta de dispositivos "vizinhos", é efetuado por roteadores e *switches* por meio dos protocolos de comunicação:

- ICMP: faz o diagnóstico da rede, relata os erros de recebimento de pacotes e no informe de características da rede.
- ARP: efetua o mapeamento dos endereços físicos (MAC) por meio do endereço lógico.
- RARP: faz o inverso do ARP, associando um endereço lógico ao físico.

Dessa forma, um roteador envia periodicamente um protocolo de atualização de vizinhança aos roteadores conhecidos e um vai enviando a atualização aos outros sucessivamente, fazendo com que a tabela lógica de endereçamento dos equipamentos continue sempre atualizada.

O mercado possui diversos tipos de roteadores, que podem apresentar funcionalidades básicas para SOHO (*Small Office Home Office* - rede doméstica ou de pequeno escritório), ou equipamentos que permitem regras de tráfego, tabelas de rotas, programação de funções e possuem "linguagens de programação" própria. Um exemplo de roteador pode ser observado a seguir:

Figura 1.21 | Roteador doméstico ou para pequeno escritório

Fonte: <https://goo.gl/rbQZRr>. Acesso em: 29 mar. 2017.

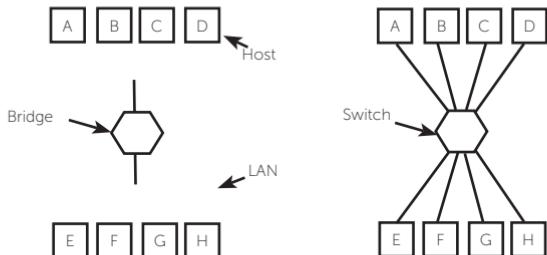
Segundo Kurose (2006), o roteador (sem fio) recebe a mensagem pela porta de entrada, repassa o pacote para o processador que efetua o roteamento, em que há a análise do endereçamento destino e encaminha para a porta de saída, na verdade apontando a interface de rede (placa ethernet).

Switch

Este tipo de equipamento é comumente encontrado em empresas, faculdades, ou seja, redes que necessitam de maior número de dispositivos. Segundo Tanenbaum (1997), quando a mensagem chega a uma das interfaces de rede, o sistema do equipamento lê o endereço destino do cabeçalho e envia para a interface apropriada. *Switches* normalmente possuem diversas portas, como pode ser observado a seguir:

Figura 1.22 | Exemplo de *switch*

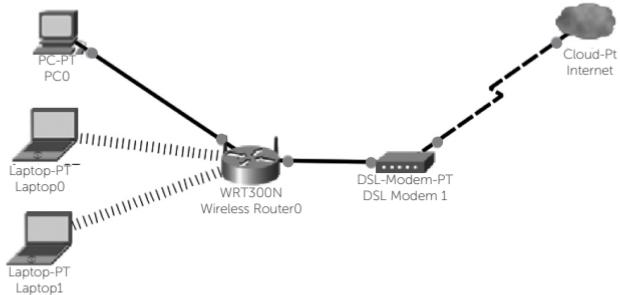
Fonte: <https://goo.gl/4y7IaH>. Acesso em: 30 mar. 2017.

A grande diferença do hub para o *switch* é o fato de que neste cada uma das portas possuem o seu domínio de colisão, já o Hub manda a mensagem para todas as portas, podendo ser encontrado com velocidades que podem variar 10/100 Mbps e 1000 Mbps, ou seja, gigabit.

O termo "Domínio de Colisão" é comumente utilizado por profissionais de redes de computadores para designar que aquelas mensagens que são replicadas para todos os dispositivos não conseguem atravessar equipamentos como o roteador e o *switch.*

Dessa forma, se uma rede possuir um roteador em cada departamento, as mensagens replicadas para os dispositivos não serão enviadas para outros departamentos, pelo limite imposto pelos equipamentos, formando assim o domínio de colisão.

Bridges (pontes)

Quando o administrador de redes necessita conectar duas redes distintas, uma solução viável pode ser utilizar as bridges (pontes), tipo de equipamento que tem características muito parecidas com o *switch*. Porém, as suas aplicações em uma infraestrutura são bem distintas, conforme pode ser observado a seguir:

Figura 1.23 | Aplicação de switch *versus* bridge

Fonte: Tanenbaum (1997, p. 255).

Enquanto o *switch* é utilizado para conectar dispositivos da rede, a bridge é empregada para interligar duas redes (LAN), mas nada impede que o administrador utilize o *switch* para interligar duas redes, desde que devidamente configurado e planejado. A vantagem de utilizar as bridges é que a sua configuração é mais simples, necessitando apenas fazer o apontamento do endereço das interfaces dos equipamentos das redes que estão sendo conectadas. Por sua vez, com o *switch,* o ganho no processamento das informações pode proporcionar melhor desempenho na comunicação entre os dispositivos de redes distintas.

Gateway

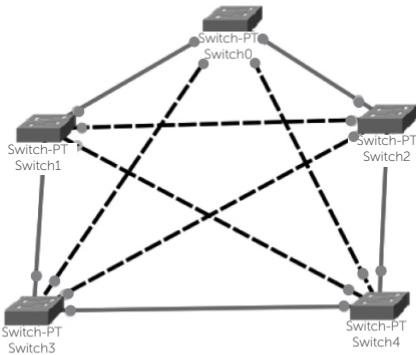
Este conceito está diretamente ligado a um termo muito utilizado por profissionais de redes de computadores, que é "borda de rede". Para a compreensão desse termo, observe a Figura 1.24 a seguir:

Figura 1.24 | Exemplo de *gateway*

Fonte: elaborada pelo autor.

A Figura 1.24 demonstra a estrutura da maioria das redes disponíveis nos lares das pessoas. Os dispositivos PC2, Laptop0 e Laptop1, ao enviar uma mensagem, utilizam como primeiro destino, de forma padronizada, o Wireless Router0, equipamento esse considerado o *gateway* da rede em questão, o que explica o nome "borda de rede", pois após o roteador, o dispositivo já está conectado à internet (rede mundial e não interna).

Tanenbaum (1997) define que o *gateway* pode ter funções específicas nas redes, dependendo do planejamento do administrador de redes, entre as quais estão:

- Direcionamento: todas as mensagens são enviadas para o nodo da rede, podendo ser roteador ou *switch*.
- Proxy: uma lista de sites a cujo acesso há ou não permissão pelos dispositivos da rede interna.
- *Firewall*: um dispositivo de segurança que verifica o conteúdo dos pacotes e efetua o bloqueio, quando há ação nociva aos serviços disponíveis na rede.

Todo dispositivo conectado em uma rede deve possuir alguns endereços lógicos, como: IP (versão 4 ou 6), máscara de rede, *gateway* e DNS, configurados.

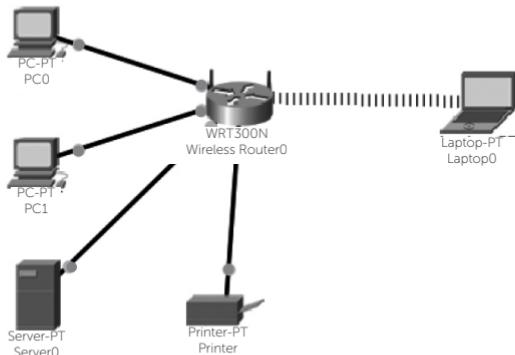
Mas de que forma os endereços lógicos podem ser verificados em dispositivo Windows, Linux, Mac ou Android? Quais devem ser os mecanismos e os comandos utilizados para esse fim?

Caro aluno, você deve ter percebido que, ao longo das seções, foram utilizadas diversas figuras que representavam o mapa das redes. Segundo Forouzan (2006), a topologia de uma rede pode ser dada como uma representação geométrica da relação dos links entre os dispositivos. Estão divididas em:

- Malha: nesta topologia, cada um dos dispositivos da rede (nodos) possui um link dedicado com os demais da rede, ou seja, efetua transferência de dados entre os dois dispositivos. Observe a seguir:

Figura 1.25 | Exemplo de topologia malha

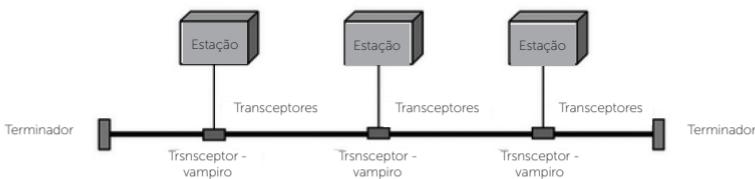
Fonte: elaborada pelo autor.

O número de links de entrada/saída dos dispositivos (nodos) é dado por (n(n-1))/2, onde n é o número de *switches* no exemplo da Figura 1.25.

Uma rede necessita de links entre todos os seis *switches* da empresa, a fim de garantir a continuidade dos seus serviços na ocorrência de falha de um ou mais dos seus links. O administrador da rede sabe que pode contar com 10 portas em cada um dos equipamentos. Porém, para desenvolver a rede com uma topologia do tipo malha, é necessário calcular o número que será utilizado, em que:

(n(n - 1)) / 2

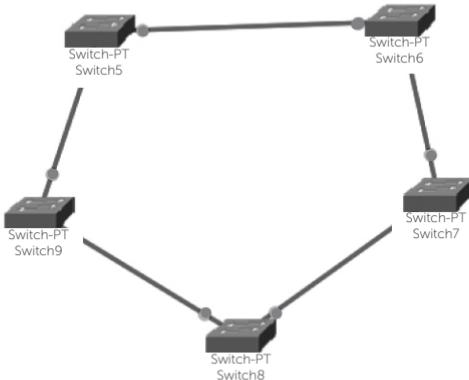
(6(6 -1)) / 2, ou seja, 15 links.

- Estrela: em geral, nesta topologia, cada dispositivo possui um link ponto a ponto com um concentrador, podendo este ser um hub, roteador ou *switch*. Observe o exemplo a seguir:

Figura 1.26 | Exemplo de topologia estrela

Fonte: elaborada pelo autor.

Os dispositivos não estão diretamente ligados entre si, porém ainda assim é possível efetuar o compartilhamento de seus recursos.

- Barramento: esta topologia é considerada ponto a ponto, pois para fazer a conexão é necessário um *backbone* (tronco central) para interligar os dispositivos, conforme pode ser observado na Figura 1.27 a seguir:

Figura 1.27 | Exemplo de topologia barramento

Fonte: Forouzan (2006, p. 11).

Na maioria das residências onde há internet cabeada, as operadoras utilizam esse tipo de topologia, em que o *backbone* da rede é o cabo instalado nos postes nas ruas e as estações são os modems que estão diretamente ligados ao tronco principal.

- Anel: cada dispositivo possui uma conexão com o seu “vizinho”; e o sinal, quando enviado, percorre o anel até que o destino seja encontrado. O formato desta topologia pode ser observado a seguir:

Figura 1.28 | Exemplo de topologia anel

Fonte: elaborada pelo autor.

A topologia em anel é uma das mais fáceis de ser instalada e configurada em razão de cada um dos nodos possuir somente duas conexões.

- Híbrida: este tipo de formato de rede pode ser encontrado em várias redes internas, por exemplo: quando há redes em estrela conectadas em um barramento (*backbone*). Se pensarmos nas redes espalhadas pelo mundo, onde há diversos tipos de topologias conectadas, podemos considerar que em nível mundial temos uma rede híbrida.

Forouzan (2006) defende que as aplicações das topologias podem variar conforme a disponibilidade de recursos e as necessidades que cada rede deve possuir. Outro fator importante é que, independentemente da topologia adotada pelo administrador de uma rede, todas elas apresentam algumas vantagens e desvantagens. Veja:

Topologia em malha: a sua vantagem é possuir links redundantes entre os nodos, o que garante maior disponibilidade de acesso aos serviços e dispositivos. A sua desvantagem é que, para fazer links redundantes, são necessários muitos cabeamentos entre os nodos.

Topologia em estrela: a vantagem deste tipo de rede é o custo, pois com um nodo é possível conectar diversos dispositivos à rede. Porém, em caso de falha do nodo, todos os dispositivos e serviços são desconectados da rede.

Topologia em barramento: esta topologia é de fácil instalação, pois é necessário um link principal (*backbone*), em que todos os dispositivos se conectam. Como desvantagem está o tempo de

detecção e recuperação de falhas, pois é necessário encontrar o ponto do *backbone* onde a conexão foi interrompida.

Topologia em anel: a sua principal vantagem é a facilidade de instalação, pois só é necessário a conexão entre os dispositivos vizinhos. A sua desvantagem é que as mensagens trafegam em uma única direção.

As redes podem ser classificadas quanto ao seu nível de abrangência, ou seja, podem ser categorizadas pelo alcance dos seus links e serviços. Segundo Forouzan (2006), as categorias estão divididas em:

- PAN (*Personal Area Network* – Rede Pessoal): são definidas as redes de curto alcance, assim como os compartilhamentos por meio do Bluetooth.
- LAN (*Local Area Network* – Rede Local): são redes locais encontradas em pequenos escritórios, residências ou campus. São projetadas para o compartilhamento de recursos computacionais (estação de trabalho). Normalmente as taxas de transmissão encontradas são de 100 Mbps a 1000 Mbps.
- MAN (*Metropolitan Area Network* – Rede Metropolitana): limita-se a uma cidade ou um distrito. Para exemplificar esse tipo de abrangência, há as redes Wi-Max (redes wi-fi de longo alcance) disponibilizadas em algumas cidades.
- WAN (*World Area Network* – Rede Mundial): permite a transmissão de qualquer tipo de dados por longas distâncias, podendo ser entre cidades, estados, países e continentes. Sua velocidade de transmissão pode variar, pois são encontrados diversos meios e capacidade de links entre os nodos.
- SAN (*Storage Area Network* – Rede de Armazenamento): rede utilizada para armazenamento de dados. Entre as abrangências encontradas esta é a mais incomum, pois as tecnologias de análise de grandes volumes de dados para aplicação comercial são recentes.

O artigo intitulado *Gerência de uma Rede Metropolitana Sem fio* traz uma discussão acerca da análise de falhas de serviços, servidores

e impressoras em uma infraestrutura de redes de condomínios empresariais, localizados na cidade de Florianópolis, onde, através do monitoramento da rede, coletaram-se diferentes tipos de falhas.

Disponível em: <https://www.researchgate.net/profile/Carlos_Westphall/publication/259494401_GERENCIA_DE_UMA_REDE_METROPOLITANA_SEM_FIO/links/0046352c4297c69680000000.pdf>. Acesso em: 26 mar. 2017.

Caro aluno, após a definição das redes pelo nível de abrangência, é possível a compreensão de dois modos como as redes podem estar estruturadas para prover os seus serviços, sendo na forma de redes distribuídas e sem fio.

Tenenbaum (2006) define que as redes distribuídas podem abranger uma área geográfica dentro de uma organização, cidade, país ou continente, tendo como objetivo interligar um conjunto de dispositivos a fim de que algumas aplicações sejam executadas aos usuários. De uma forma mais abrangente, as redes podem ser definidas como geograficamente distribuídas (WAN), em que diversas LANs estão interligadas.

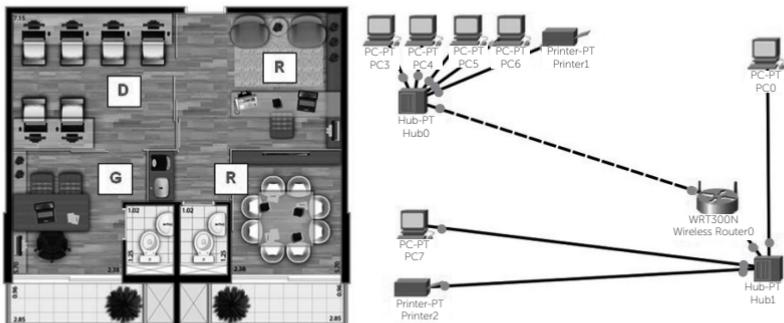
A internet sem fio se popularizou na maioria dos lares e locais de grande fluxo de pessoas, como terminais, restaurantes, praças, etc. A tecnologia parece nova, porém a sua primeira aplicação data de 1901 (Marconi) segundo Tanenbaum (1997), tendo sido utilizada para transmissão de um navio para o litoral por código Morse. Nas redes atuais há dois tipos de aplicações:

- LAN sem fio: são sistemas dotados por um modem de rádio e uma antena para a transmissão dos dados. A sua abrangência em área livre deve ficar restrita a um prédio, *campus* ou escritório, dependendo de quantos retransmissores são utilizados na topologia. O padrão de comunicação utilizado para as LANs é conhecido por IEEE 802.11, ou seja, wireless ou wi-fi.
- WAN sem fio: são antenas de transmissão potentes o suficiente para cobrir uma rede geograficamente distribuída, com uma abrangência de uma cidade por exemplo. As

velocidades podem variar conforme as características técnicas de transmissão e recepção do sinal. No Brasil, as operações pela tecnologia conhecidas por WI-Max se iniciaram no ano 2008; as primeiras cidades foram: Belém, Belo Horizonte, Brasília, Curitiba, Fortaleza, Goiânia, Porto Alegre, Recife, Rio de Janeiro, Salvador, São Luis e São Paulo (Fonte: <http://www.teleco.com.br/wimax.asp>, acesso em: 2 mar. 2017).

Sem medo de errar

Com o projeto em andamento na filial em Campinas, ao longo da semana os colaboradores relataram alguns problemas de lentidão na rede. Isso ocorreu em razão do cascateamento com os hubs.

Para resolver esses problemas, a empresa adquiriu os seguintes equipamentos:

- 1 servidor (modelo *generic*) e 1 notebook para a sala do gerente de projetos.
- 1 *switch* (modelo *generic*) e 3 notebooks para a sala de desenvolvimento.
- Notebooks conectados na wi-fi do roteador da sala de reunião.

As seguintes alterações devem ser feitas na rede:

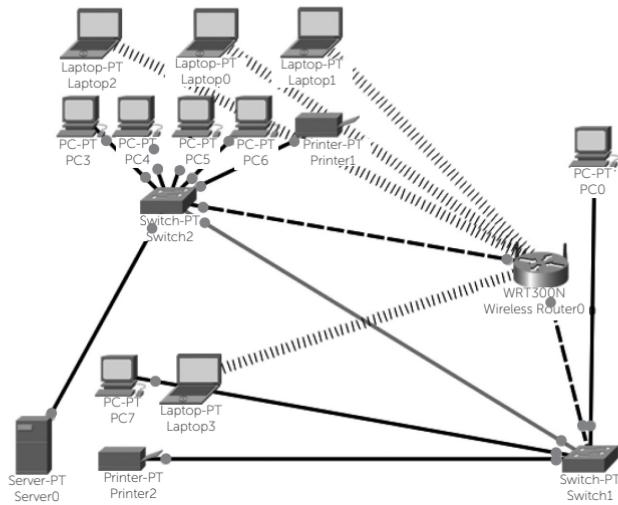
1. Os hubs da rede devem ser substituídos pelo *switch*.

2. Os switches devem ser conectados um ao outro por fibra óptica.

3. Um Servidor deve ser instalado na sala do gerente de projetos (não é preciso configurar serviço algum).

4. Os notebooks devem ser conectados no roteador já instalado na sala de reunião.

As alterações devem ser feitas na rede modelada no software de simulação de redes Cisco Packet Tracer, na Seção 1.2. Lembrando de que a planta baixa e a topologia configurada inicialmente são apresentadas a seguir:

Figura 1.29 | Topologia da empresa

Fonte: <https://goo.gl/jbSs8z>. Acesso em: 4 jul. 2017.

Para isso, devem ser feitos os seguintes passos:

- Exclua os dois hubs da rede e instale um *switch (generic)* no lugar.
- Para suprir o número de portas necessárias no *switch,* clique no *switch* → *Physical* → Desligue o equipamento (On/Off) → instale a placa arrastando a opção "PT-SWITCH-NM-1-CE" → Ligue o equipamento (On/Off).
- Faça a conexão entre os *switches*: opção *Connections* → Fiber. Ligue os dois *switches*.
- Para instalar o servidor na sala do gerente, escolha a opção *End Device* → 3ª Opção de *Generic* (Server - PT) e conecte o servidor no *switch* na sala de desenvolvimento.
- Instale um notebook na sala do gerente e três na sala de desenvolvimento. Para instalar a antena wi-fi no notebook, clique no notebook → *Physical* → Desligue o equipamento (On/Off) → desinstale a placa "PT-LAPTOP-NM-1CFE" → Instale a placa "WPC300N" → Ligue o equipamento (On/Off).

Com as alterações efetuadas na da empresa, a topologia segue como na Figura 1.30 a seguir:

Figura 1.30 | Nova Topologia da empresa

Fonte: elaborada pelo autor.

Dessa forma, com a substituição dos hubs, a rede ganhará em desempenho, possibilitando que os tempos de execução dos serviços de redes não sofram atrasos. Além disso, com a chegada dos dispositivos com conexão wi-fi, o roteador da sala de reuniões passou a ser utilizado, com a possibilidade de fornecer conexão a novos colaboradores e visitantes por meio da rede sem fio.

Avançando na prática

Cálculo de número de links para redundância

Descrição da situação-problema

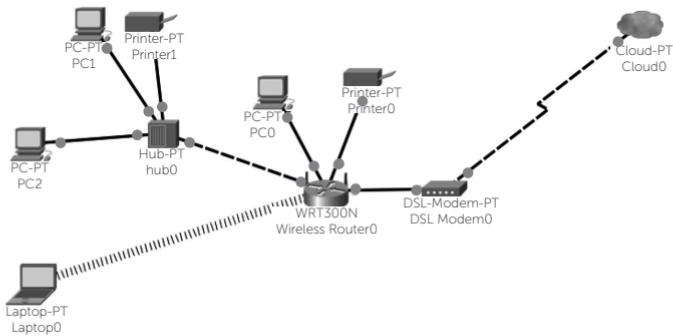
O departamento de TI necessita mudar a topologia da rede de estrela para malha. Criar links redundantes pode garantir o compartilhamento dos seus recursos e serviços e a consequente otimização do tempo dos colaboradores. Em sua estrutura foram colocados dois *switches* no armário de dispositivos (Rack) e um *switch* em cada um dos 11 departamentos distribuídos no prédio da companhia.

Para resolver essa questão, é necessário efetuar o cálculo de quantos links são necessários para formar uma topologia em malha.

Resolução da situação-problema

A empresa possui dois *switches* localizados no Rack e onze *switches* espalhados pelos departamentos, totalizando assim treze switches. Para o cálculo da quantidade de links, usa-se a expressão (n(n-1))/2, em que n representa o número de *switches*. Dessa forma,

(13(13-1))/2 =

(13*12)/2 =

156/2 = 78

Ou seja, serão necessários 78 links, ou ainda, serão utilizadas seis portas por *switch*, possibilitando ao administrador de redes prever quantas portas serão necessárias para atender às necessidades de cada um dos departamentos.

Faça valer a pena

1. Um escritório de advocacia possui um especialista em cada área (família, civil e criminal) para atender às necessidades de seus clientes. Graças à utilização das impressoras e da internet para consulta dos processos on-line, os equipamentos têm que ser configurados corretamente. A topologia utilizada no escritório tem as características apresentadas a seguir:

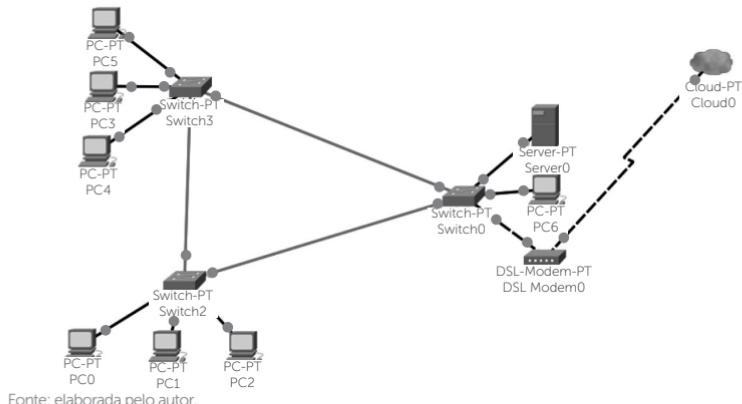
Figura 1.31 | Topologia do escritório de advocacia

Fonte: elaborada pelo autor.

Com base na topologia apresentada, assinale a alternativa que descreva o nome do equipamento que deve ser o gateway da rede.

a) DSL Modem0.
b) Wireless Router0.
c) Cloud0.
d) Hub0.
e) PC0.

2. As topologias existentes são categorizadas segundo o seu nível de abrangência, o que permite ao administrador de rede ter uma visão mais ampla dos possíveis caminhos que a mensagem percorre para ir da origem até o destino. As necessidades de abrangência da rede variam conforme as necessidades e os recursos disponíveis para a sua estruturação.

Com base nas categorias de rede, faça a associação entre as duas colunas a seguir:

(A) PAN	( ) Rede de uma praça de alimentação
(B) LAN	( ) Transmissão de arquivos entre dois smartphones via bluetooth
(D) WAN	( ) Wi-max instalado para utilização dos moradores da cidade
(E) SAN	( ) Cloud para armazenamento de projetos
	( ) Servidores de jogos on-line

Assinale a alternativa com a sequência CORRETA de associações, de cima para baixo:

a) B – C – E – D – A.
b) D – B – A – C – E.
c) E – D – B – A – C.
d) B – A – C – E – D.
e) D – E – C – B – A.

3. A empresa Zap possui os seguintes equipamentos em sua topologia:

Figura 1.32 | Topologia Empresa Zap

Fonte: elaborada pelo autor.

Os serviços disponibilizados pelo servidor (Server0) são de extrema importância para as aplicações utilizadas.
Para a garantia de alta disponibilidade, o administrador de redes decidiu que a rede deve ser estruturada em topologia em malha entre os *switches* e servidor.

Assinale a alternativa com o número de portas necessárias para efetuar links redundantes entre os equipamentos mencionados:

a) 2 links.

b) 10 links.

c) 4 links.

d) 8 links.

e) 6 links.

Referências

CARISSIMI, A. **Redes de Computadores**. Instituto de Informática UFRGS. Porto Alegre: Bookman, 2009.

COMER, D. E. ***Computer and Networks Internet with Internet Applications,*** São Paulo: Artmed, 2007..

FOROUZAN, A. **Comunicação de Dados e Redes de Computadores**. Porto Alegre: Bookman, 2006.

KUROSE, J. F. **Redes de Computadores e a Internet**: Uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley 2006.

TANENBAUM, A. S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus, 1997.

Protocolos e serviços de rede

Convite ao estudo

Agora que você já possui os conhecimentos básicos acerca dos aspectos históricos de telecomunicações, da importância da comunicação de dados nos dias atuais e dos equipamentos necessários para estruturar uma rede de computadores, será possível progredir, a fim de compreender a importância dos protocolos nos serviços encontrados nas redes de computadores espalhadas ao redor do planeta.

A compreensão dos aspectos técnicos, no tocante às redes de computadores e aos protocolos envolvidos na comunicação, permitirá que você consiga prover serviços e efetuar o compartilhamento dos recursos disponíveis.

Nesta unidade, será possível entender:

- As características e a importância do modelo de referência OSI na comunicação de dados.
- A maneira para identificar e classificar os serviços de rede e a hierarquia dos protocolos.
- A forma pela qual os protocolos TCP/IP possibilitaram que as redes geograficamente distribuídas pudessem se comunicar de forma confiável.

Dessa forma, alguns serviços podem ser configurados para oferecer aos usuários funções importantes das redes de computadores.

Caro estudante, para que você possa planejar uma rede com os serviços essenciais para continuidade dos negócios, faz-se necessário compreender como o modelo de referência

OSI fez com que houvesse a padronização dos protocolos de comunicação e hardwares envolvidos nas redes de computadores. Desse modo, facilitou-se o entendimento das técnicas de endereçamento de redes, que são de extrema importância para que os usuários possam acessar os serviços disponíveis. Pronto para mais um desafio?

Seção 2.1

Protocolos e serviços de rede

Diálogo aberto

O entendimento dos aspectos técnicos e as características do modelo de referência OSI permitirão a compreensão de como os protocolos de comunicação foram desenvolvidos e propiciarão prover os serviços utilizados diariamente (como mensagens instantâneas, e-mail, acesso a sites, serviços de *streaming* de vídeo e jogos on-line, entre diversos outros), possibilitando, assim, que você possa configurar os serviços necessários nas redes.

O sucesso no desenvolvimento da rede de computadores na filial em Campinas da empresa. rendeu a sua equipe mais uma indicação, dessa vez um escritório de engenharia civil.

A empresa 2@@ está localizada na cidade do Rio de Janeiro. As atividades desenvolvidas por seus engenheiros são relacionadas a projetos de edificação de prédios comerciais, e os seus clientes são construtoras de grandes edifícios empresariais. Dessa forma, prestar serviços para o escritório pode ser uma grande responsabilidade.

Em um dos projetos, foi solicitado pelo cliente que o edifício tivesse uma rede de sensores que permitisse gerar e transmitir informações de temperatura, umidade relativa e presença.

Para tal tarefa, a empresa 2@@ solicitou um relatório em que fossem descritas as funções que cada camada no modelo de referência OSI teria que desempenhar caso fosse decidido que o protocolo de comunicação implementado nos sensores seria proprietário, ou seja, desenvolvido por alguma empresa de desenvolvimento de software.

Caro aluno, desenvolver um relatório com a descrição das funções de cada uma das camadas do protocolo OSI, para uso futuro no projeto da empresa 2@@ vai possibilitar que você compreenda a importância do modelo de referência OSI e da forma como os dados são formatados, organizados, transmitidos/recebidos, interpretados e utilizados pelo usuário.

Não pode faltar

Caro aluno, imagine que você tenha sido enviado para trabalhar em um projeto com algumas pessoas que não falam o mesmo idioma. Se os gestores não encontrarem um idioma que todos possam falar, a comunicação pode se tornar uma grande ameaça na execução do projeto. Padronizar a forma de as pessoas se comunicarem pode garantir que as informações sejam passadas e compreendidas corretamente.

Os processos necessários para adquirir uma padronização podem se diferenciar conforme o tipo de aplicação ou a entidade que fará os estudos e as análises. Essas entidades que efetuam esse tipo de trabalho estão espalhadas pelos continentes, com destaque para:

- ISO (*Internacional Organization for Standardization*) – organização não governamental responsável pela padronização. É dividida em:
    - ◊ ANSI (*American National Standards Institute*).
    - ◊ ABNT (Associação Brasileira de Normas Técnicas).
    - ◊ ANFOR (Associação Francesa).
    - ◊ DIN (Associação Alemã).
- EIA (*Eletronic Industries Association*) – grupo que visa padronizações das transmissões elétricas.
- IEEE (*Institute of Eletrical and Eletronics Engineers*) – a maior organização internacional de desenvolvimento e padronização nas áreas de engenharia elétrica e computação.
- ITU-T (*Telecommunication Standardization Sector*) – entidade responsável pela padronização dos assuntos relacionados a telecomunicações.

As redes de computadores necessitavam de uma forma padrão para poder se comunicar. Em razão disso, ocorreu um importante processo evolutivo quando a ISO (*International Standards Organization*), em um esforço com o seu grupo de engenheiros, instituiu o modelo de referência OSI (*Open Systems Interconnection* – Sistemas Abertos de Conexão).

O problema de falta de padronização atingia não somente os protocolos de comunicação (parte lógica), mas também os

hardwares desenvolvidos pelos fabricantes. Por exemplo: se uma empresa decidisse adquirir equipamentos IBM, jamais poderia ter em sua topologia algum dispositivo DEC, pois não haveria compatibilidade entre as duas marcas.

Segundo Tanenbaum (1997), o desejo da ISO era desenvolver uma forma universal de interconexão de sistemas abertos. Para isso, foi desenvolvido um modelo em sete camadas, que deveria atender aos seguintes requisitos:

- Cada camada deve executar a função à qual foi destinada.
- A função das camadas deve ser escolhida em razão dos protocolos que foram padronizados.
- Os limites entre as camadas devem ser escolhidos a fim de minimizar os esforços ao fluxo das mensagens pelas interfaces.
- O número de camadas deve ser do tamanho suficiente para alocar todas as funcionalidades possíveis nas redes.

Em 1981, a ISO conseguiu reunir algumas empresas para dar início ao projeto de padronizar a forma de comunicação das redes de computadores. Finalmente, em 1984, foi criado um padrão para os hardwares e softwares de diversos fabricantes, assim como o modelo de referência para que fossem desenvolvidos os protocolos, que viriam a interagir com os dispositivos.

Reflita

Ao observarmos os objetos que utilizamos diariamente, vamos perceber que existe um padrão, por exemplo: os pneus utilizados nos automóveis, o formato dos livros, a caixa de leite, entre diversos outros. Isso acontece porque os países possuem órgãos regulamentadores a fim de garantir a segurança dos consumidores.

Com relação às redes de computadores, qual é a vantagem de padronizar a forma de se comunicar?

Segundo Tanenbaum (1997), o modelo de referência OSI efetua todos os processos necessários para que ocorra a transmissão de dados, fazendo com que as camadas (*layers*) nele existentes

efetuem a divisão dos processos lógicos. Isso significa que um determinado fabricante tem a liberdade de desenvolver o seu protocolo, desde que utilize como referência os parâmetros determinados pelo OSI, o que é conhecido como "Protocolo Proprietário".

Dessa forma, a ISO desenvolveu o modelo de referência OSI (*Open Systems Interconnection* – Sistemas Abertos de Conexão), um marco para o desenvolvimento dos protocolos de comunicação, utilizados nos serviços consumidos diariamente pela internet. A arquitetura do modelo é apresentada a seguir:

Figura 2.1 | Modelo de Referência OSI

7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace
1	Física

Fonte: elaborada pelo autor.

Logo no início, o modelo de referência foi imposto aos fabricantes pelo governo americano, porém o mercado reagiu com desconfiança. No Brasil, o governo agiu da mesma maneira, mas também sem sucesso. Isso ocorria porque em vários países já havia no mercado alguns modelos proprietários (ex.: IBM) que eram funcionais e atendiam às necessidades das aplicações disponíveis nas redes.

Com o passar do tempo, por volta de 1984, os fabricantes hardwares e desenvolvedores de softwares entenderam que o modelo proposto em camadas tinha como intuito permitir a interoperabilidade entre equipamentos de diferentes origens, o que poderia dar uma vantagem competitiva em nível de mercado, além de permitir parcerias e novos desenvolvimentos.

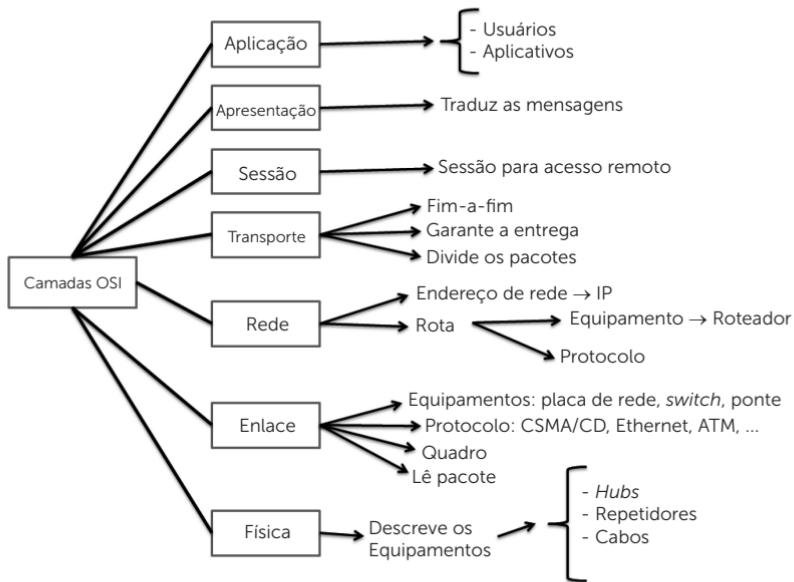
O modelo de referência não é exatamente a arquitetura dos protocolos de rede, mas sim uma referência de como os protocolos devem ser estruturados. Tanenbaum (1997) define assim as características e funcionalidades de cada uma das camadas:

- **Camada física:** nesta camada está definida a forma de transmissão dos bits pelo canal de comunicação. Deve ser determinada a voltagem que representa os bits 0s e 1s, o tempo de duração dos bits (em nanossegundos) e o método de transmissão (simplex, half-duplex ou full-duplex). Entre os equipamentos descritos nesta camada estão os *hubs*, repetidores e cabos.
- **Camada de enlace:** os dados provenientes da camada física são transformados em quadros, o que facilita a detecção de erros, para que não seja repassada à camada de rede. Os dados são divididos em algumas centenas de quadros para assim serem transmitidos. Entre os equipamentos utilizados nesta camada estão as placas de redes (endereço de MAC), os *switches* e *bridges*.
- **Camada de rede:** a forma como os dados são roteados da origem até o seu destino é definida nesta camada. As tabelas referentes às rotas podem ser estáticas, e os dispositivos vizinhos são responsáveis por manter a tabela de roteamento atualizada. Como em alguns casos, o caminho mais curto não é o mais rápido, pois os links podem possuir diferentes velocidades. O controle do congestionamento (gargalo de rede) também é efetuado nessa camada.

O endereçamento IP-Internet Protocol (veja mais detalhes na Seção 2 da Unidade 3) opera nesta camada. O seu principal equipamento, o roteador, é o responsável por “ler” o endereço de origem/destino e encaminhar os pacotes na rota correta.

- **Camada de transporte:** os dados provenientes da camada de sessão ao chegar nesta camada são divididos em unidades menores. No entanto, o mais importante é a garantia de que os pacotes chegarão corretamente ao seu

destino. Também é determinado o tipo de serviço que a camada de sessão deve utilizar, sendo o mais comum a conexão ponto a ponto.

- **Camada de sessão:** os computadores que estão separados geograficamente são conectados nesta camada. São gerenciados diversos serviços, controle de acesso, sincronização e a verificação de status da conexão.
- **Camada de apresentação:** esta camada analisa a semântica e a sintaxe dos dados transmitidos, ou seja, os diferentes serviços utilizados. Antes de serem intercambiados, analisa-se o tipo de dado, para que seja utilizada a codificação correta durante a conexão. Um exemplo do serviço de tradução (codificação/decodificação) dos dados que pode ser utilizado é o ASCII (*American Standard Information Interchange*).
- **Camada de aplicação:** local em que os usuários se comunicam com o computador responsável por prover a disponibilidade dos recursos no dispositivo destino. Nesta camada estão definidos os navegadores (IE, Firefox, Safari, etc.), os servidores web (Apache, Netscape, e-mail) e de banco de dados (MySql, Oracle, Postgree).

Pesquise mais

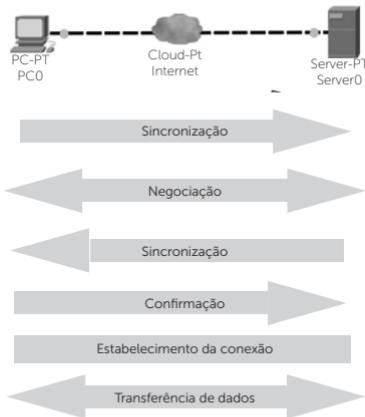
O texto de Marcia Guimarães intitulado *Os anões e o Modelo OSI* faz uma analogia entre os sete anões do filme *Branca de Neve e os Sete Anões* e o Modelo de Referência OSI.

Disponível em: <https://testeassuntos.blogspot.com.br/2008/09/os-anoes-e-o-modelo-osi_9.html>. Acesso em: 9 maio 2017.

Para melhor compreender o modelo de referência OSI e as suas respectivas funções, observe a Figura 2.2 a seguir:

Figura 2.2 | Modelo de Referência OSI e as suas funções

Fonte: elaborada pelo autor.

Após a aceitação do modelo de referência OSI pelas empresas desenvolvedoras de hardware, em pouco tempo o mercado já dispunha de dispositivos que seguiam normas e padrões. Podemos perceber isso nos equipamentos como roteadores, smartphones e notebooks, que permitem acesso aos recursos em qualquer infraestrutura de rede.

O acesso remoto é uma ferramenta muito utilizada pelos profissionais de redes de computadores. Ela permite que máquinas que não estejam no mesmo local sejam acessadas com a utilização de um terminal *Shell* (cmd no Windows). Dessa forma, é possível gerenciar de forma remota banco de dados, servidores de impressão, arquivos, sistemas e websites. Esse tipo de serviço é utilizado na camada aplicação do modelo de referência OSI.

Controle de fluxo

Segundo Tanenbaum (1997), a integridade dos dados é efetuada na camada de transporte. Esse mecanismo garante que as requisições efetuadas pelos usuários sejam confirmadas, recebidas e atendidas. Para a compreensão desse mecanismo, observe a Figura 2.3 a seguir.

Figura 2.3 | Mecanismo de controle de fluxo

Fonte: Filippetti (2008, p. 45).

Na Figura 2.3, o computador à esquerda deseja acessar um site que está disponível em um servidor em algum provedor. Inicialmente o computador faz uma requisição ao servidor, então ocorre a negociação, quando são verificados o meio de transmissão e o protocolo, processo conhecido também como *handshaking*, ou seja, aperto de mãos. O servidor, então, autoriza a sincronização. Assim que o computador confirma o recebimento, é estabelecida a conexão e se iniciada a transmissão dos dados. Tal processo acontece para que ocorra a garantia de recebimento e o controle das transmissões. Para isso:

- Qualquer segmento que não recebe a confirmação de recebimento é retransmitido.
- Os segmentos são reconstruídos na sua sequência inicial quando recebidos pelo computador.
- O mecanismo de envio e recebimento faz a gerência do fluxo, a fim de evitar perda de dados e gargalos na rede.

Kurose (2006) define que, para que o modelo de referência OSI pudesse funcionar de forma eficiente, deveria ser proposto um mecanismo de confirmação das mensagens entre os dispositivos (*acknowledgement*). A técnica deve garantir que os dados não sejam perdidos ou duplicados, ou seja, ao enviar uma mensagem para um dispositivo, este deve retornar uma mensagem de confirmação de recebimento. Daí dá-se o nome de confirmação positiva de retransmissão (*acknowledgement with retransmition*).

Exemplificando

Gargalos na rede mundial de computadores são fenômenos bem comuns, já que os serviços que são providos diariamente podem sofrer falhas ou perdas. Um exemplo de gargalo ocorre nos últimos dias de entrega da declaração de imposto de renda, quando o grande número de chegadas simultâneas de informações pode deixar o serviço indisponível, embora o problema também possa ocorrer por falha na aplicação.

Gargalos em redes de computadores são responsáveis pela degradação dos serviços, razão pela qual, ao se pensar na estruturação das topologias, o administrador deve procurar mecanismos que garantam a disponibilidade das aplicações.

Interação entre as camadas

Segundo Tanenbaum (1997), as quatro camadas inferiores (física, enlace, rede e transporte) possuem nomes específicos para o tratamento dos dados:

- Camada física → bits.
- Camada de enlace → Quadro/*frame*.
- Camada de rede → Pacote/Datagrama.
- Camada de transporte → Segmento.

No processo de transmissão nas redes, é utilizada a técnica de encapsulamento das mensagens. De maneira análoga, é como se os dados fossem embrulhados para depois serem transmitidos. O modelo de referência OSI indica que uma camada de transmissão se

comunique com a sua camada "irmã" do dispositivo receptor e esse processo é repetido até que as camadas de sessão, apresentação e aplicação possam interpretar e exibir o conteúdo dos dados ao usuário.

Kurose (2006) define os passos necessários para que ocorram o envio e a recepção das mensagens. Para isso, vamos tomar o mesmo exemplo utilizado na Figura 2.3, quando um computador tenta acessar um site localizado em um servidor.

Através da *camada de aplicação*, o browser efetua a solicitação de acesso ao site. Em seguida, o formato é lido (*camada de aplicação*) e encaminhado à *camada de sessão*, que vai efetuar o gerenciamento da conexão. Os dados são encapsulados na *camada de transporte*, ganhando o nome de **segmento**. Em seguida, a *camada de rede* adiciona os endereços de origem e destino e os encapsula, tornando-se assim um **pacote**. Chegando à *camada de enlace*, segmentam-se os dados, aos quais se atribui o nome de **quadro**. Por último, os quadros são transformados em **bits** na *camada física* e em seguida enviados pelas redes até o seu destino.

Ao chegar ao destino, é efetuado o processo inverso pela pilha. Processo depois do qual é enviada a resposta ao usuário para que o site seja acessado.

Caro aluno, lembre-se de que esta é apenas uma descrição dos processos que o modelo de referência OSI fornece para a estruturação dos protocolos de comunicação. OSI não é protocolo, mas sim um guia de desenvolvimento para comunicação em redes de computadores.

Sem medo de errar

A empresa 2@@, um escritório de engenharia localizado na cidade do Rio de Janeiro, é responsável por desenvolver projetos de edificação de grandes prédios comerciais. Atualmente, os colaboradores estão envolvidos em um projeto que visa a atender uma necessidade específica de um cliente, que tem como objetivo a instalação de sensores que forneçam informações como presença, umidade do ar e temperatura.

Para isso, a empresa 2@@ solicitou um relatório com a descrição das funções que cada camada do modelo de referência OSI deve

desempenhar caso seja decidido o desenvolvimento de um protocolo proprietário que permita a operacionalização das funções solicitadas pelo cliente. Veja a seguir um exemplo de relatório para este caso:

Sr. Diretor da empresa 2@@,

Para atendimento das necessidades de prover a comunicação dos sensores que permitirão informações como presença do usuário nas dependências do prédio, temperatura ambiente e umidade relativa do ar, caso seja decidido pelo desenvolvimento de um protocolo proprietário, este deve permitir que:

- O gerenciamento ocorra de forma individual nas camadas.
- As alterações ocorridas em uma das camadas não alterem o estado e/ou funcionamento das demais.
- Seja possível a implementação ou adaptação em dispositivos de diversos fabricantes de sensores, permitindo assim a interoperabilidade.

Dessa forma, as camadas do modelo de referência OSI devem desempenhar as seguintes funções:

Camada física: devem ser especificadas as interfaces de entrada e saída dos sensores, as especificações elétricas e o modo como os bits serão movimentados.

Camada enlace: os erros devem ser detectados nesta camada, porém não é efetuada a correção. Deve ser adicionado um campo de aviso de erro no quadro (nome do encapsulamento).

Camada rede: o endereço lógico de cada sensor deve ser definido nesta camada.

Camada transporte: deve garantir uma conexão ponto a ponto com o dispositivo que vai receber os dados gerados pelos sensores.

Camada sessão: deve efetuar a conexão das portas lógicas dos sensores (campo que deve permitir a alteração conforme determinar o fabricante do sensor).

Camada apresentação: deve tratar a semântica das mensagens e tradução dos dados enviados pelos sensores.

Camada aplicação: permite uma interface para leitura e interpretação dos dados gerados pelos sensores.

Dessa forma, sugerimos que as indicações das camadas do modelo de referência OSI para o desenvolvimento de um protocolo sejam implementadas no máximo de dispositivos de fabricantes e modelos diversos, a fim de garantir a interoperabilidade.

Caro aluno, o desenvolvimento de um relatório com as funções que as camadas devem realizar para as necessidades da empresa empresa 2@@ permitiu a compreensão das características e da aplicabilidade de cada uma das camadas do modelo de referência OSI, ainda com a preocupação de como os dados são formatados para permitir a comunicação.

Avançando na prática

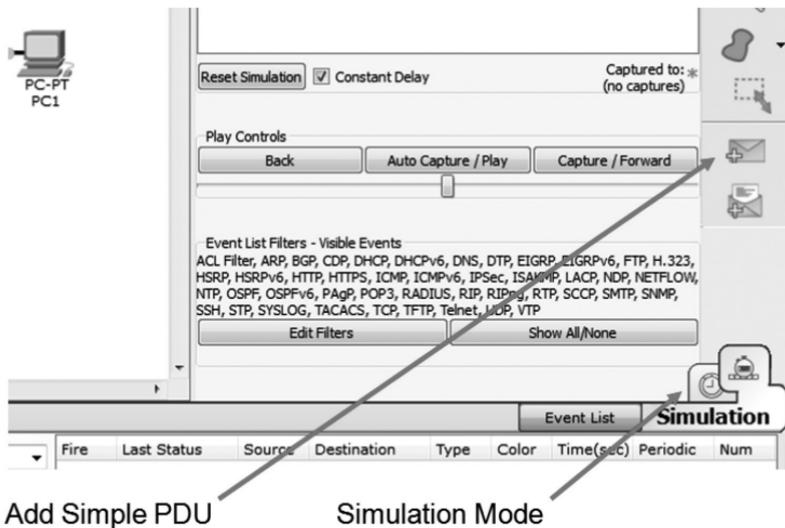
Demonstração do Modelo OSI

Descrição da situação-problema

Uma empresa farmacêutica deseja desenvolver um chat que possibilitará aos vendedores realizar chamadas com o gerente de vendas para concessão de desconto nas vendas diárias. No entanto, para isso, inicialmente é necessário ter uma forma visual de como é o comportamento das camadas do modelo de referência OSI ao se enviar uma mensagem de um computador para outro.

Com base nisso, o diretor de TI solicitou que fosse utilizado o software de simulação de redes Packet Tracer na topologia experimental que pode ser observada a seguir:

Figura 2.4 | Rede experimental

Fonte: elaborada pelo autor.

Para isso, deve-se estruturar a rede representada na Figura 2.4 para enviar mensagens de um computador ao outro e, posteriormente, efetuar a demonstração visual do modelo OSI no Packet Tracer.

Resolução da situação-problema

Após realizar a conexão dos dispositivos na topologia experimental, clique no PC0, na aba "Desktop", "*IP Configuration*", e marque a opção "DHCP". Repita o mesmo procedimento no PC1.

No canto inferior direito, clique em “*Simulation Mode*”. Em seguida, selecione “*Add Simple PDU*” e clique em cima do PC0 (origem) e depois no PC1 (destino), como pode ser observado na Figura 2.5 a seguir:

Figura 2.5 | Teste na rede experimental

Fonte: elaborada pelo autor.

Depois disso, na janela aberta, clique em *Auto Capture / Play* e, a qualquer momento, selecione os envelopes que estão sendo enviados, em que a interação nas camadas do modelo OSI pode ser observada.

Faça valer a pena

1. Para os produtos e serviços consumidos diariamente, é exigido, antes de serem disponibilizados, que sejam efetuados testes para a comprovação de eficácia, segurança para o consumidor, entre outros fatores. Tais ensaios realizados em laboratórios devem ser conduzidos por órgãos específicos de cada área de conhecimento.
A forma de se comunicar e os protocolos de comunicação foram padronizados pela ISO (*International Standards Organization*), o que possibilitou um avanço na área de telecomunicações.

Quando se planeja padronizar um produto, um processo ou serviços, uma das vantagens é o ganho de qualidade, segurança e confiabilidade por parte dos consumidores. Assinale a alternativa que descreve a intenção ao desenvolver um modelo de referência para a comunicação de dados.

a) O desenvolvimento de um modelo em camadas isoladas, que não permite a interação entre elas, para que ocorra a comunicação de forma independente.

b) Um modelo somente para a construção dos hardwares de rede, pois isso, por si só, já garantiria a padronização na comunicação entre os dispositivos.

c) Efetuar o controle da comunicação, permitindo os países mais ricos vigiarem as mensagens trocadas.

d) Obter um modelo com os serviços bem definidos nas camadas, aberto para a utilização, que permitisse a comunicação por meio de diversos dispositivos.

e) Obter o prêmio Nobel em Engenharia, pois esse status permitiria aos membros da ISO (*International Standards Organization*) mais patrocínios em seus projetos.

2. Observe o texto a seguir:

A ISO (*International Standards Organization*), no ano de 1981, reuniu engenheiros de algumas empresas ligadas ________________________, acadêmicos e profissionais de tecnologia da informação, a fim de padronizar a comunicação nas redes de computadores. Após anos de estudos e testes, em 1984 os hardwares e ____________________ de comunicação possuíam um modelo de referência denominado OSI. O modelo foi dividido em _________________ camadas, com funções bem definidas em cada uma delas.

Para conhecer como e porque um produto foi desenvolvido, é necessário conhecer as motivações e os aspectos históricos envolvidos nas suas características técnicas. Nesse contexto, assinale a alternativa que complete as lacunas corretamente.

a) à administração – serviços – sete.

b) ao governo – protocolos – seis.

c) a telecomunicações – protocolos – sete.

d) a telecomunicações – serviços – oito.

e) à eletrônica – meios de – seis.

3. Os serviços consumidos diariamente como o WhatsApp, Facebook, aplicativos de compra, entre outros tantos, necessitam de protocolos para prover a comunicação. Esses protocolos utilizados nas redes de computadores foram estruturados com base no modelo de referência OSI, desenvolvido em sete camadas, conforme apresentado a seguir:

Modelo de Referência OSI

7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace
1	Física

Fonte: elaborada pelo autor

Segundo Tanenbaum (1997), as quatro camadas inferiores (física, enlace, rede e transporte) possuem nomes específicos para o tratamento dos dados. Nesse contexto, relacione as duas colunas seguintes:

(A) Camada física
(B) Camada de enlace
(C) Camada de rede
(D) Camada de transporte

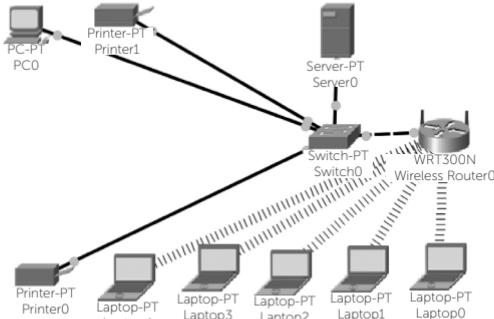
(   ) Segmento.
(   ) Bits.
(   ) Quadro / *frame*.
(   ) Pacote / datagrama.

Assinale a alternativa com a sequência correta de associação, de cima para baixo.

a) B – A – C – D.
b) C – B – D – A.
c) D – C – A – B.
d) D – A – B – C.
e) A – D – B – C.

Seção 2.2

O modelo de referência ISO/OSI

Diálogo aberto

Caro aluno, na Seção 2.1 você pôde compreender o modelo de referência OSI e a importância que ele teve para que houvesse uma padronização na forma de prover a comunicação entre os dispositivos. Com isso, será possível estudar:

- Os protocolos empregados para que diversos serviços de rede sejam utilizados diariamente.
- A maneira como eles são organizados e hierarquizados.
- As interfaces utilizadas nos serviços.
- A forma como são classificados os serviços das redes.

Tais conhecimentos possibilitarão ao profissional de redes de computadores organizar e gerenciar os serviços que devem ser providos, a fim de atender às necessidades de comunicação e de compartilhamento de recursos.

A empresa 2@@ faz projetos de engenharia para grandes empreendimentos comerciais e, em seu dia a dia, necessita compartilhar os desenvolvimentos em andamento e aqueles que já foram concluídos entre todos os membros da equipe de desenvolvimento. Para isso, foi sugerido alocar um site com os projetos no servidor HTTP encontrado na topologia, conforme pode ser observado a seguir:

Figura 2.6 | Topologia empresa 2@@

Fonte: elaborada pelo autor.

Com isso, será necessário configurar os serviços HTTP e DNS no servidor instalado na sala do gerente (rede desenvolvida do Packet Tracer).

Com a configuração do servidor HTTP, será possível hospedar os projetos de engenharia. Por sua vez, o DNS vai resolver o nome de domínio para possibilitar que os dispositivos encontrem o site *www.projetoseng.com.br*, escolhido para acesso às informações necessárias para auxiliar os engenheiros nas atividades de desenvolvimento.

Tais configurações auxiliarão você a responder como os protocolos de comunicação utilizados nas redes de computadores podem prover os serviços utilizados diariamente.

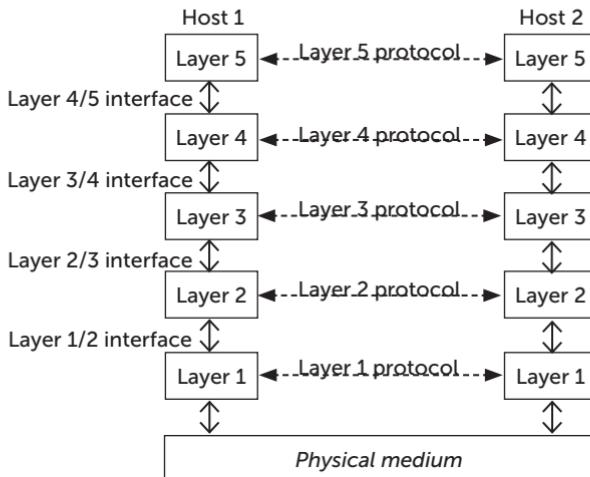
Vamos encarar esse desafio e aumentar o seu conhecimento acerca das redes de computadores?

Não pode faltar

Caro estudante, agora que você já possui conhecimentos sobre o modelo de referência OSI visto na seção anterior, será possível, então, compreender como os protocolos são utilizados nas redes para prover os serviços nas redes de computadores.

Forouzan (2008, p. 19) define que, em redes de computadores, "protocolo é sinônimo de regra". Ao enviar uma mensagem para qualquer dispositivo encontrado na rede mundial de computadores, tanto o emissor quanto o receptor precisam utilizar um protocolo com que as duas partes concordem. Por meio de um conjunto contendo várias regras, é possível efetuar o controle da comunicação. A arquitetura do protocolo deve possuir os elementos-chave:

- Sintaxe: averigua-se o formato que os dados possuem, ou seja, a ordem como são apresentados. Por exemplo: um protocolo utiliza oito bits para o endereço do emissor, oito bits para o endereço do receptor e 16 bits para o conteúdo da mensagem.
- Semântica: analisa-se qual é a característica de cada seção de bits, como cada padrão se comporta e qual deve ser a decisão tomada. Por exemplo: o conteúdo dos pacotes para

acessar um site tem a semântica diferente da dos pacotes destinados a *streaming* de vídeo.

- Timing: refere-se ao tempo durante o qual as mensagens são enviadas, em que se verifica: quando a mensagem deve ser enviada e a que velocidade. Por exemplo: uma mensagem é enviada a uma velocidade de 100 Mbps, porém o receptor só pode recebê-la a 1 Mbps.

Hierarquia e interfaces dos protocolos nos serviços de redes

Segundo Tenenbaum (1997), assim como determina o modelo de referência OSI, os protocolos são organizados em pilha ou camada, porém em todas as redes a função primordial é fornecer serviços às camadas superiores.

Para isso, o mecanismo utilizado faz com que a camada "n" de um dispositivo se comunique com a camada "n" de outro dispositivo. Basicamente, o protocolo efetua a "negociação" entre as partes para que seja provida a comunicação, conforme pode ser observado na Figura 2.7 a seguir:

Figura 2.7 | Camadas e interfaces

Fonte: Forouzan (2008, p. 46).

Quando os dados são transferidos, cada camada processa o seu serviço respectivo. Para que isso ocorra, a cada par de camadas existe

uma interface, responsável por definir as operações e os serviços que a camada inferior tem que encaminhar à camada superior.

Ao projetar as interfaces nas redes, a carga de trabalho das informações que devem ser passadas entre as camadas é reduzida, pois, dessa forma, só é necessário oferecer o mesmo conjunto de serviços entre os dispositivos que estão se comunicando.

Os protocolos utilizados nas redes de computadores estão diretamente ligados aos serviços utilizados nas redes de computadores diariamente. Por exemplo, ao utilizar um aplicativo em um smartphone, são necessários diversos protocolos como o TCP/IP, DNS, NTP, entre outros, para que seja provido algum tipo de serviço.

Nesta seção vamos nos concentrar nos protocolos que operam na camada 7 (aplicação) do modelo de referência OSI, pois na Seção 2.3 serão tratados os demais protocolos da camada de rede e transporte. Dessa forma, por meio dessa divisão, será possível maior compreensão do funcionamento e das principais características dos protocolos que agem em ambas as camadas. Segundo Tanenbaum (1997), estão definidos os seguintes protocolos:

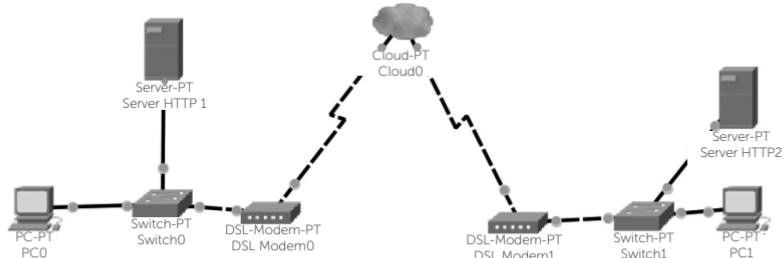
- **HTTP**: trata-se de um protocolo utilizado para acessar conteúdo web na rede mundial de computadores. Permite que ocorra a transferência ponto a ponto entre clientes e servidores, de serviços do tipo elástico e *streaming* (multimídia), conforme pode ser observado na Figura 2.8 a seguir:

Figura 2.8 | Servidor HTTP

Fonte: elaborada pelo autor.

Para compreensão do funcionamento do servidor HTTP, um exemplo ocorre quando um computador efetua uma solicitação para acessar um site alocado em um Servidor HTTP quando digitada a URL (*Uniform Resource Locator* – Localizador Padrão de

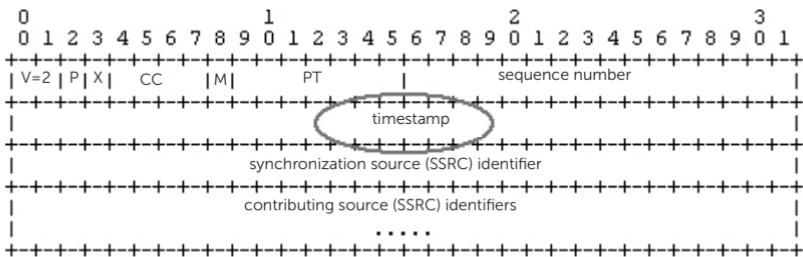
Recursos), o endereço do site disponível em algum dispositivo na rede mundial de computadores. Ao receber a solicitação, o servidor envia a resposta, sendo possível ao usuário visualizar o conteúdo por meio de um navegador web.

Para hospedagem de sites, sistemas web, jogos on-line, entre outras aplicações, o mercado possui diversas empresas que disponibilizam hospedagem gratuita. No Quadro 2.1 a seguir é demonstrado o endereço do *host* (nome dado à hospedagem web) e os respectivos serviços disponibilizados.

Quadro 2.1 | Hosts de hospedagem gratuitos

Host	Serviços
000webhost.com	HTTP, E-mail, Banco de dados e FTP.
freehostia.com/hosting.html	HTTP e E-mail.
hostinger.com	HTTP, E-mail e FTP.
Servidorgratuito.com	HTTP, E-mail, Banco de dados e FTP.

Fonte: elaborado pelo autor.

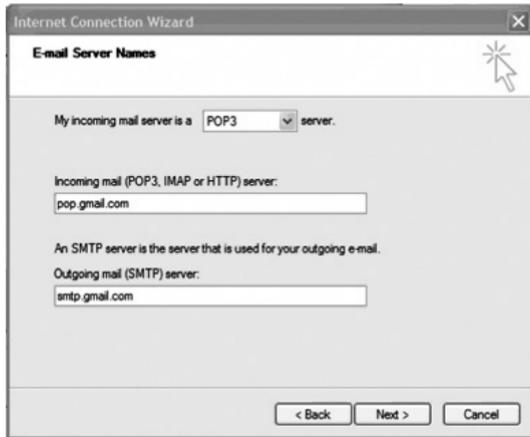
- **SMTP**: é a sigla para *Simple Mail Transfer Protocol* (Protocolo Simples de Transferência de E-mail). É o protocolo utilizado para efetuar a transferência de e-mail de um servidor para outro, conforme observado a seguir:

Figura 2.9 | Transação SMTP

Fonte: elaborada pelo autor.

No exemplo acima, o usuário A do "PC0" possui uma conta de e-mail localizada no "Server HTTP 1"; por sua vez, no "PC1", o usuário B possui uma conta de e-mail no "Server HTTP 2". Quando o usuário A escreve uma mensagem ao usuário B, esta primeiramente é enviada para o "Server HTTP 1" e, depois disso, o protocolo SMTP se encarrega de transferi-la para o "Server HTTP 2", possibilitando, assim, que o usuário B consiga acessar a mensagem.

Para que isso ocorra, o acesso aos e-mails pode ser efetuado via web, usando o HTTP. Este servidor HTTP, por sua vez, acessa o servidor SMTP, onde estão alocadas as mensagens.

- **SSH (Secure SHell)**: este protocolo é utilizado para efetuar acesso remoto em outro dispositivo, por meio de um terminal, assim como o prompt de comando do DOS. A grande diferença para as outras técnicas (telnet e RSH) de acesso remoto está relacionada com a segurança. Ao fazer um acesso remoto em um dispositivo, a transmissão de dados recebe uma criptografia que pode variar conforme o algoritmo de encriptação das mensagens, a fim de garantir a integridade do que é compartilhado.
- **RTP**: trata-se de um protocolo de transporte utilizado na camada de aplicação para prover serviços *streaming* de áudio e vídeo. A sua sigla significa *Real-Time Transfer Protocol*, ou seja, protocolo de transferência de tempo real. Com esse mecanismo, é feito o transporte das mensagens fim a fim dos dados do tipo multimídia. O cabeçalho do protocolo possui um campo específico com informações sobre o tempo, conforme demonstrado na Figura 2.10 a seguir:

Figura 2.10 | Cabeçalho RTP

Fonte: <https://goo.gl/9iQVbq>. Acesso em: 2 maio 2017.

O protocolo utiliza o campo *timestamp* para compensar o atraso dos pacotes. Essa compensação faz com que não ocorra a degradação dos serviços.

- SIP *(Session Initiation Protocol):* apesar de este protocolo não pertencer à camada de aplicação e sim ser definido na camada de sessão, vale ressaltar o seu grau de importância para os serviços multimídia. Este protocolo é responsável pela criação, modificação e finalização de sessões de transferência de arquivos de serviços multimídia. O seu funcionamento é idêntico ao do HTTP, ou seja, uma conexão do tipo cliente/servidor. Para o gerenciamento das sessões, o protocolo deve conter:

◊ Localização do usuário: determina a localização do dispositivo dentro de uma topologia.

◊ Capacidade do usuário: determina a capacidade de transmissão do serviço *streaming*.

◊ Disponibilidade do usuário: este procedimento confirma se o dispositivo está ativo após a sua localização.

◊ Configuração de chamada: são definidos os parâmetros para estabelecimento da conexão, conforme as características técnicas da rede e do tipo de serviço.

◊ Controle de chamada: após o estabelecimento da conexão, é gerenciada a chamada, a transferência de dados e o encerramento.

- POP3: essa expressão pode ser traduzida como protocolo de escritório postal (*Post Office Protocol*), já disponível em sua terceira versão. Esse protocolo permite que o usuário descarregue as mensagens que estejam localizadas em um servidor de e-mail em seu dispositivo.

Quando as operadoras de internet não ofereciam conexões com velocidades mais altas, alguns programas, como Outlook ou Thunderbird, eram utilizados para esse fim. Observe na área central do Outlook Express os e-mails carregados:

Figura 2.11 | Exemplo do uso do Protocolo POP3

Fonte: <https://goo.gl/wy9Sg1>. Acesso em: 16 jul. 2017.

Essa ferramenta permite o recebimento das mensagens, porém não o seu envio.

- **IMAP:** assim como ocorre com o POP3, este protocolo sincroniza as mensagens alocadas em um servidor de e-mail, porém se mantém conectado a fim de sincronizar as mensagens recebidas, em tempo real.
- **NTP:** o *Network Time Protocol* (Protocolo de Tempo de Redes) tem como função sincronizar os relógios dos servidores, roteadores e computadores das redes. Para fazer com que ocorra a sincronia, os servidores NTP são estruturados por uma topologia hierarquizada em camadas, entre as quais existe um mecanismo de consulta de tempo para o ajuste preciso. Por sua vez, os dispositivos solicitam a atualização do tempo para os servidores. Essas associações podem ser do tipo:

◊ Permanente: é configurado manualmente o tempo no servidor para que seja referenciado em todos os dispositivos da rede.

◊ Priorizável: assim como o permanente, é configurado manualmente, porém com a possibilidade de possuir mais servidores referenciando o tempo aos dispositivos.

◊ Transitórias: são servidores disponíveis na rede mundial que atualizam o tempo dos dispositivos encontrados nas redes.

Reflita

Para que o protocolo RTP funcione corretamente e garanta que os serviços *streaming* funcionem, é necessário que o servidor NTP esteja atualizando o tempo dos dispositivos, evitando atrasos e a degradação dos serviços. Em redes de computadores ocorre dependência entre os protocolos para que sejam providos os serviços.

Com exceção do RTP e do NTP, quais protocolos utilizados nas redes possuem dependências entre si?

Caro aluno, por ter um papel de extrema importância na rede mundial de computadores, o protocolo **DNS** (*Domain Name System* – Sistema de Nomes de Domínios) necessita de um pouco mais de detalhes.

Para isso, Forouzan (2008) define que esse protocolo tem como função principal efetuar a tradução do número IP (*Internet Protocol*) para o nome de domínios, dentro de um servidor DNS, conforme exemplo no Quadro 2.2 a seguir:

Quadro 2.2 | Nome de domínio e o IP correspondente

Nome de domínio	IP correspondente
kroton.com.br	87.86.214.62
google.com.br	216.58.202.131
teleco.com	64.14.55.148
cert.br	200.160.7.17

Fonte: elaborado pelo autor.

A hierarquia dos domínios é dividida em três categorias diferentes:

- Domínio genérico: são definidos os registros conforme o segmento do site, podendo estes ser: .com, .net, .org, .edu, .gov, entre outros.
- Domínio de países: é utilizada a abreviatura com dois caracteres para identificar em qual país o domínio foi registrado, podendo ser: br (Brasil), us (Estados Unidos), ar (Argentina), entre outros.

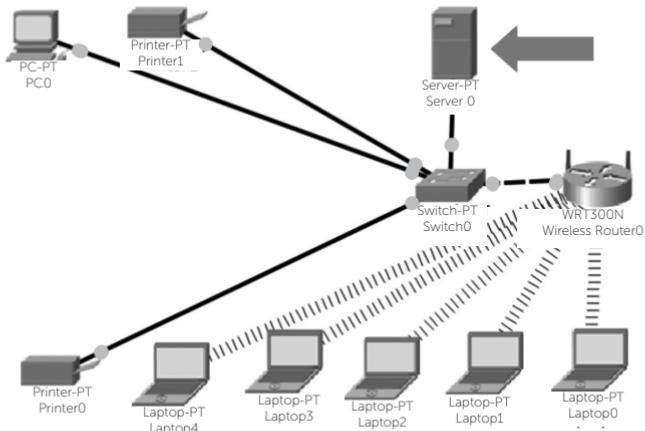
- Domínio reverso: faz o processo reverso à consulta ao servidor DNS. Quando um servidor recebe uma solicitação, é feita uma consulta em sua "tabela", que por sua vez encaminha a solicitação do cliente, apontando para o servidor relacionado ao endereço digitado pelo usuário, sendo utilizado o endereço IP.

Pesquise mais

Ao iniciar um projeto de um sistema web ou a construção de um site, o desenvolvedor necessita fazer uma consulta de disponibilidade para que o provedor possa ser registrado no endereço escolhido no servidor DNS do provedor. No Brasil as consultas e registros são feitos pelo <https://registro.br/> (acesso em: 17 ago. 2017).

Para a compreensão de todo o processo para adquirir um endereço, assista ao vídeo disponível em: <https://www.youtube.com/watch?v=gZRYDxWuYpk&feature=youtu.be>. Acesso em: 3 maio 2017.

Dessa forma, o resolvedor do nome de domínio basicamente precisa responder como uma aplicação do tipo cliente/servidor, que tem a capacidade de mapear e encaminhar as solicitações de acesso a sites por meio do endereço ou número IP fornecido.

Caro estudante, ao longo desta seção nós estudamos diversos protocolos da camada de aplicação. No entanto, existem diversos outros como o Telnet, POP, NIS, NFS, LDAP, etc. Embora eles desempenhem algumas funções, nos atemos aos protocolos mais relevantes nos serviços utilizados nas redes de computadores.

As redes de computadores são compostas por servidores, links físico e lógico, meios de transmissão e diversos serviços como: e-mail, *streaming*, *e-commerce*, entre outros. Ou seja, as arquiteturas disponíveis nas redes devem ser implementadas observando-se o mecanismo de especificações das camadas e interfaces, regra que pode ser aplicada tanto para os softwares, quanto para os hardwares utilizados nas comunicações.

Sem medo de errar

Para auxiliar os engenheiros a ter acesso aos projetos anteriores e àqueles que estão em andamento, foi sugerido um site para hospedar tais informações. Porém, para isso, a sua equipe deve configurar os serviços de HTTP e DNS no servidor já instalado na topologia, conforme indicado na Figura 2.12 a seguir:

Figura 2.12 | Servidor da empresa 2@@

Fonte: elaborada pelo autor.

O nome do endereço escolhido para o site pela gerência da empresa 2@@ é o www.projetoeng.com.br.

Configuração do Servidor HTTP (em destaque na Figura 2.12):

- Após clicar no servidor, acesse a aba "Desktop", procure a opção "*IP Configuration*" e anote o número "*IP Address*" (Ex.: 192.168.0.7).
- Em seguida acesse a aba "*Services*", clique na opção HTTP e ative (*on*) os serviços de HTTP e HTTPS.

Configuração do servidor DNS (em destaque na Figura 2.12):

- Ainda no servidor, acesse a aba "*Service*", clique na opção "DNS" e configure:

◊ Em "*Name*", coloque o endereço do site: www.projetoeng.com.br.

◊ Em “*Address*”, coloque o número do IP do servidor (Ex.: 192.168.0.7).

- Em seguida, clique em “*ADD*” para gravar a configuração e, por último, ative o serviço DNS (*on*).

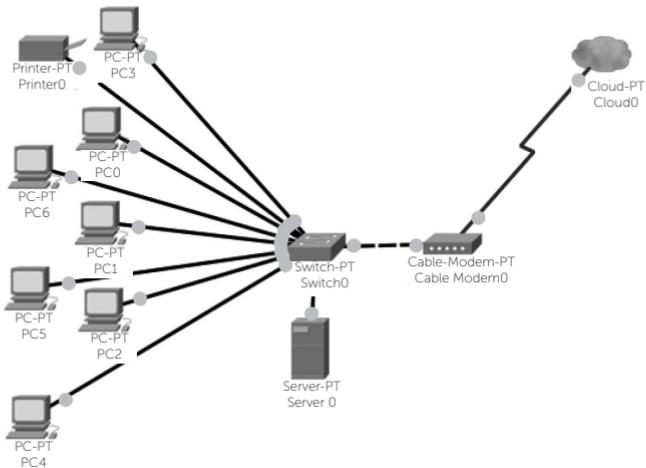
Configuração dos computadores/notebooks da empresa 2@@ :

Para que os computadores acessem o site, deve-se fazer “apontamento” para o servidor DNS. Para isso, em TODOS os computadores de ambas as redes, deve ser feito o seguinte procedimento:

- Após clicar no computador/notebook, selecione a aba “Desktop” e a opção “*IP Configuration*”.
- O número do “*DNS Server*” está em branco: para configurá-lo, marque a opção “*Static*” e novamente marque a opção “DHCP”; o número do servidor DNS que foi apontado quando o roteador foi configurado vai aparecer em “*DNS Server*” (Ex.: 192.168.0.7).

Teste de acesso ao site:

A fim de testar as configurações, o Packet Tracer possui um site instalado. Para isso, escolha um dos computadores, clique na aba “Desktop” e selecione a opção “*Web Browser*”. No navegador, digite no campo “URL” o endereço do site de treinamento (www.projetoeng.com.br).

As configurações realizadas nas redes possibilitaram a compreensão da importância dos protocolos de redes para que os serviços necessários no dia a dia possam ser providos.

Avançando na prática

Servidor DHCP para uma rede

Descrição da situação-problema

Uma rede de computadores necessita de diversas interfaces para acomodar todos os dispositivos necessários na topologia apresentada a seguir:

Figura 2.13 | Topologia da rede

Fonte: elaborada pelo autor.

Como não existe um roteador com o DHCP, o responsável por atribuir o endereçamento IP (*Internet Protocol*) aos dispositivos da rede, é necessário efetuar a configuração do serviço no "Server0". Quais alterações a configuração do DHCP pode promover em uma rede como essa apresentada?

Resolução da situação-problema

Para configurar o serviço de DHCP em um servidor, o administrador de redes basicamente deve determinar: o endereço do *Gateway*, do DNS (quando necessário ou disponível) e os endereços inicial e final que serão atribuídos aos dispositivos.

Tais configurações na topologia apresentada possibilitarão que os dispositivos recebam automaticamente os endereçamentos necessários para acessar os recursos compartilhados, como a impressora e o acesso à internet.

Faça valer a pena

1. Para as pessoas enviarem uma encomenda pelos serviços do correio, é necessário efetuar alguns procedimentos padronizados pela ECT (Empresa de Correios e Telégrafos), como: endereço de origem e destino, caixa ou pacote, taxa de postagem, entre outros.

De maneira análoga, as redes de computadores possuem algumas regras de acesso e envio das suas mensagens para que estas consigam ser transportadas por diversos meios, sendo os protocolos utilizados como sinônimo de regra na comunicação de dados segundo Forouzan (2008).
As redes necessitam de diversos protocolos para prover serviços essenciais na comunicação de dados, tanto nas residências, quanto em empresas. Mas, para isso, a arquitetura do protocolo deve possuir três elementos-chave. Observe os três itens a seguir:

I. Sintaxe: a análise é feita no conteúdo que a mensagem possui.
II. Semântica: é analisado o formato do dado com que se deseja prover a comunicação.
III. *Timing*: refere-se ao tempo de que as mensagens necessitam para ser enviadas.
Assinale a alternativa CORRETA:

a) Somente o item II é verdadeiro.
b) Somente os itens I e III são verdadeiros.
c) Somente o item III é verdadeiro.
d) Somente os itens II e III são verdadeiros.
e) Somente o item I é verdadeiro.

2. A padronização na forma de se comunicar, proporcionada pelo advento do modelo de referência OSI, e os protocolos desenvolvidos proporcionaram que dispositivos de diferentes fabricantes pudessem enviar e receber as mensagens. Os serviços disponíveis nas redes, como mensagens instantâneas, *streaming* de vídeo, jogos on-line, etc., dependem de um ou mais protocolos para que cumpram o seu objetivo.
Para que os dispositivos possam acessar os serviços disponíveis nas redes, é necessário que eles tenham um endereçamento lógico relacionado à sua interface de rede. Tal endereço pode ser obtido de duas formas:
Manual: são atribuídos os endereços manualmente pelo administrador da rede.
Automática: o protocolo ________ atribui os endereços automaticamente aos dispositivos da rede.

Assinale a alternativa que complete o nome do protocolo CORRETO:
a) DNS.
b) HTTP.
c) DHCP.
d) IMAP.
e) NTP.

3. Em 2007 os especialistas previam o crescimento de 300% na utilização de internet móvel até o ano de 2017, porém o aumento esperado ocorreu em meados de 2015. A previsão é que em 2020 o número de usuários possa ser quatro vezes maior do que o atual.

Para atender a toda essa demanda, existe uma infraestrutura numerosa de equipamentos e serviços. Os profissionais de redes de computadores necessitam conhecer diversas técnicas e ferramentas a fim de garantirem o acesso às aplicações com segurança e qualidade.

Para testar o acesso ao servidor web, o administrador de redes digitou o nome de domínio do site no navegador. Em seguida ele fez o mesmo procedimento com o endereço desse site. Tanto no endereço quanto no nome de domínio, o site que abriu no navegador foi o mesmo.

O protocolo que tem a capacidade de revolver o nome de domínio para proporcionar acessos aos serviços e às aplicações web disponíveis nas redes.

Com base nisso, indique (V) para as afirmações verdadeiras ou (F) para as falsas:

(   ) Os domínios genéricos definem o seguimento de um site.

(   ) O domínio dos países identifica em que país ocorreu o registro de um site.

(   ) Os domínios dos países podem ser: .com, .net, .org, .edu, .gov, entre outros.

(   ) O domínio reverso faz a consulta inversa ao servidor DNS.

(   ) Os domínios genéricos podem ser: .br, .us, .ar, entre outros.

Assinale a alternativa com a sequência correta de indicações, de cima para baixo:

a) V – F – V – F – V.
b) F – V – V – V – F.
c) F – F – V – F – V.
d) V – V – F – V – F.
e) V – F – V – V – V.

Seção 2.3

O protocolo TCP/IP

Diálogo aberto

Caro estudante, após configurar os servidores DNS e HTTP, os engenheiros conseguiram, por meio de um site, fazer consultas a fotos e documentos de projetos passados e em andamento.

A empresa 2@@ é uma empresa que desenvolve projetos de edificações para grandes prédios comerciais e, diariamente, os engenheiros precisam compartilhar arquivos dos projetos em desenvolvimento, documentações e planilhas de cálculos. Normalmente esses arquivos são compartilhados via e-mail, porém, graças ao tamanho dos arquivos, tal tarefa tem sido um problema nos projetos.

Para solucionar o problema de compartilhamento de arquivos, um servidor FTP deve ser configurado na rede. Isso vai permitir que os colaboradores possam fazer download e upload dos arquivos que são gerados diariamente, para a condução dos seus projetos. Para realizar essa tarefa, o serviço deve ser configurado no servidor que se encontra na topologia da empresa 2@@.

O conjunto de serviços que o protocolo TCP/IP proporciona faz com que as redes ganhem diversas funcionalidades.

Dessa forma, você deve utilizar o Cisco Packet Tracer para configurar o serviço FTP na rede desenvolvida no para a simulação feita na empresa 2@@. Ao desenvolver tais alterações na rede modelada, você vai compreender a importância do protocolo TCP/IP para prover os serviços nas redes de computadores.

Você está pronto para buscar conhecimentos para resolver mais esse desafio?

Não pode faltar

Diariamente utilizamos algum meio computacional para nos comunicarmos, seja por mensagens instantâneas, e-mail, videoconferência, seja ainda por uma postagem em redes sociais.

Historicamente, o homem sempre pesquisou e desenvolveu meios para tornar o ato de conseguir passar mensagens eficiente, rápido, barato e seguro.

Nesta seção você vai conhecer os aspectos históricos, as características e as funções das camadas do protocolo TCP/IP. Com isso será possível compreender como os protocolos proveem os serviços que estamos acostumados a utilizar, por meio de aplicações, para entretenimento, trabalho ou estudos.

Filippetti (2008) afirma que o padrão TCP/IP foi desenvolvido pelo DOD (Departamento de Defesa Americano) para que, em caso de guerras, houvesse a garantia da integridade das mensagens enviadas. Isso é compreensível, uma vez que o envolvimento em diversos conflitos ao longo dos tempos fez com que o exército necessitasse de técnicas relacionadas à comunicação.

A arquitetura do protocolo TCP/IP foi desenvolvida em quatro camadas, e um conjunto de processos (aplicações) é utilizado para prover diversos serviços. Para melhor compreensão das suas camadas, observe a Figura 2.14, em que é efetuada uma comparação entre as camadas do modelo de referência OSI e o protocolo TCP/IP:

Figura 2.14 | Mapeamento do Modelo OSI *versus* TCP/IP

OSI		TCP/IP
Aplicação		Aplicação
Apresentação		
Sessão		
Transporte		*Host-to-host*
Rede		Internet
Enlace		Acesso à rede
Física		

Fonte: Filippetti (2008, p. 128).

Para isso, podemos definir a função de cada uma das camadas do protocolo TCP/IP como:

- Camada de aplicação (*Application Layer*): nesta camada define-se como os programas vão se comunicar com as diversas aplicações disponíveis nas redes. Ainda é de responsabilidade dessa camada efetuar o gerenciamento da interface com que o usuário vai interagir com a aplicação.

- Camada de transporte (*Host-to-host Layer*): é idêntica à camada de transporte do modelo de referência OSI, ou seja, responsabiliza-se por prover, gerenciar e encerrar uma conexão ponto a ponto. Ao efetuar o gerenciamento da conexão, visa-se garantir a integridade dos dados, pelo sequenciamento dos pacotes segmentados para efetuar o envio/recebimento das mensagens.
- Camada de rede (*internet layer*): tem o mesmo objetivo da camada de rede do modelo de referência OSI, sendo responsável por definir o endereçamento dos dispositivos por meio do IP e garantir o roteamento dos pacotes através das redes.
- Camada de acesso à rede (*network access layer*): desempenha a mesma função das camadas de enlace e a física do modelo de referência OSI. É efetuado o monitoramento do trafego e é analisado o endereçamento de hardware antes da transmissão pelo meio físico.

O modelo de referência OSI é uma base para sistematização dos principais protocolos utilizados nas redes de dados. No entanto, o TCP/IP surgiu no ano de 1979; e o modelo de referência OSI, em 1984. Apesar disso, o protocolo TCP/IP mantém as características necessárias referenciadas para que os dispositivos possam se comunicar.

Podemos destacar algumas semelhanças entre o modelo OSI e o protocolo TCP/IP:

- A divisão é feita em camadas.
- As camadas de transporte e rede são equivalentes.
- A comutação de pacotes é definida no modelo e efetuada no protocolo.
- Os profissionais de redes necessitam conhecer ambos.

Com a concepção do protocolo TCP/IP foi possível o desenvolvimento de diversos serviços encontrados nas redes de dados.

Caro estudante, existem diversos protocolos definidos nas camadas do protocolo TCP/IP, porém, ao longo desta seção, vamos definir alguns exemplos, conforme pode ser observado adiante:

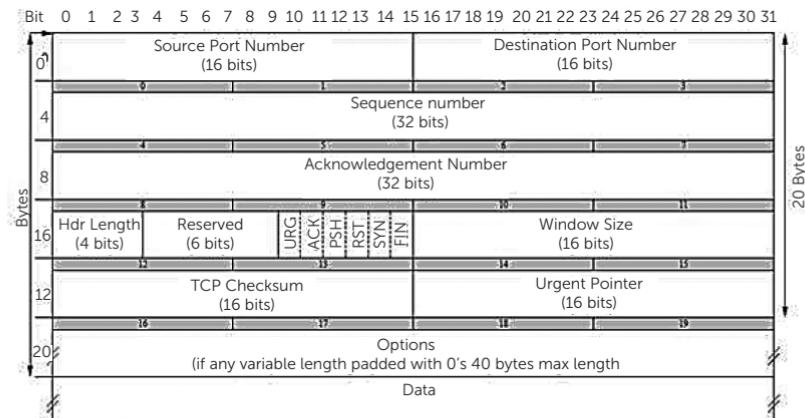
Na camada de aplicação:

- Telnet: o seu significado é *telephone network*, tendo como função principal efetuar a conexão remota utilizando um terminal (no Windows o *prompt* de comando).
- FTP (*File Transfer Protocol*): é um protocolo que tem como objetivo efetuar a transferência de arquivos entre dois dispositivos.

Para efetuar a transferência de arquivos, muitos desenvolvedores de sistemas utilizam o protocolo FTP, dentro de um programa para efetuar upload dos ficheiros necessários para o funcionamento do desenvolvimento (aplicação web ou site).

Um exemplo de um programa utilizado para esse fim é o “FileZilla”, um software de código aberto que pode ser utilizado em sistemas operacionais Windows, Linux e Mac.

- SMTP (*Simple Mail Transfer Protocol*): trata-se de um protocolo responsável por gerenciar a distribuição de e-mail aos usuários.
- SNMP (*Simple Network Management Protocol*): é um protocolo muito utilizado por administradores de redes, pois ele pode ser um aliado na coleta e na manipulação de algumas informações geradas. Possibilita ao responsável pela rede saber se algum evento inesperado ocorre (Ex.: falha de um link entre dois *switches*).

Na camada de transporte:

- TCP (*Transmission Control Protocol*): a principal função deste protocolo é quebrar as mensagens provenientes da camada de aplicação, em segmentos, e numerá-las. Quando recebe o fluxo das mensagens, o dispositivo faz a reconstrução a partir dos números adicionados no cabeçalho do protocolo. Além dessa função, o TCP deve:

◊ Confirmar o recebimento: ao enviar uma mensagem, o dispositivo receptor deve confirmar o recebimento, pois, dessa forma, é possível reenviar os segmentos não recebidos.

◊ Estabelecer a conexão: antes de iniciar o envio das mensagens, o protocolo TCP deve estabelecer a conectividade, já que esse tipo de *transmissão é orientada à conexão*.

◊ Escolher um caminho confiável: apesar de ser full-duplex, o protocolo através das tabelas de roteamento procura sempre o melhor caminho para transporte de suas mensagens.

Segundo Tanenbaum (1997), todas essas características encontradas no protocolo TCP/IP é que fazem dele o de maior confiabilidade na transmissão das mensagens. Por isso, esse protocolo é utilizado para transmissões do tipo elástico, ou seja, aquelas requisições em que a confirmação do recebimento das mensagens é essencial para que não ocorra a degradação do serviço. Exemplo: quando um usuário acessa um site, se não houver a confirmação do recebimento de todos os segmentos, a página pode não ser montada, ou ser montada com falhas.

Para compreensão da estrutura do protocolo TCP, observe a seguir:

Figura 2.15 | Cabeçalho TCP

Fonte: Stevens (1994, p. 34).

Filippetti (2008) define que cada campo do cabeçalho tem as respectivas funções:

Souce port number **(porta de origem):** número da porta lógica onde a aplicação está localizada.

Destination port number **(porta destino):** número da porta lógica onde está a aplicação do dispositivo destino.

Sequence number **(número sequencial):** número que sequencia os segmentos transmitidos/recebidos.

Acknowledgement number **(número de confirmação):** número de confirmação de conexão.

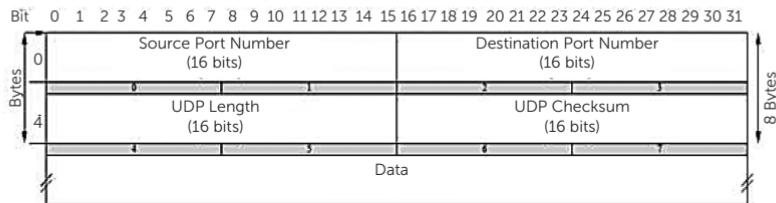
Header lenght **(comprimento do cabeçalho):** define o comprimento do cabeçalho TCP.

Reserved **(reservado):** campo reservado.

Code bits: campos responsáveis por gerenciar o início e o encerramento das conexões.

Windows **(janela):** tamanho da janela de dados que mede a capacidade de recebimento do remetente.

TCP checksum: este campo faz checagem de controle de erros (redundante).

Urgent pointer **(marcação de urgência):** determina os dados críticos, aqueles com maior prioridade na transmissão.

Option **(opção):** onde é definido o tamanho máximo do segmento.

Data **(dados):** os dados transmitidos.

- UDP (*User Datagram Protocol*): é considerada uma versão simplificada do protocolo TCP. Dessa forma, não utiliza tanto a largura da banda disponível, pois não efetua a confirmação do recebimento das mensagens, razão pela qual é considerada como um protocolo de transmissão não confiável.

Para compreensão da estrutura do protocolo UDP, observe a seguir:

Figura 2.16 | Cabeçalho TCP

Fonte: Stevens (1994, p. 70).

Segundo Tanenbaum (1997), o protocolo UDP recebe as mensagens provenientes das camadas superiores, quebra-as em segmentos e as transmite, porém a numeração para sequenciar não é adicionada. Ao receber as mensagens, caso um segmento não seja recebido, o protocolo UDP ignora o fato. Um exemplo de utilização são os serviços do tipo *streaming*.

Observe o Quadro 2.3 a seguir com a comparação dos protocolos da camada de rede:

Quadro 2.3 | TCP versus UDP

TCP	UDP
Serviço orientado à conexão	Serviço sem conexão
Garante a entrega por meio da confirmação de recebimento, pois os dados são sequenciados.	Não garante o recebimento, pois os dados não são sequenciados.
O programa que utiliza o TCP possui um transporte confiável.	A garantia de recebimento do software que utiliza o protocolo UDP deve ser garantida pelo programa.
Transmissão lenta e necessita de maior largura de banda.	Transmissão rápida e ocupa menos largura de banda.
Comunicação ponto a ponto.	Suporte a comunicação *multicast*.

Fonte: Stevens (1994, p. 70).

Caro aluno, dessa forma pode-se concluir que os protocolos da camada de transporte (TCP e UDP) possuem aplicabilidades diferentes. O TCP é indicado para conexões do tipo elástico, em que é necessária a confirmação de recebimento e retransmissão em caso de falha para que não ocorra a degradação dos serviços. Por sua vez, o protocolo UDP é indicado para os serviços *streaming*, em que não é necessária

a confirmação do recebimento das mensagens, não ocorrendo dessa forma a retransmissão de falhas de envio/recebimento.

Reflita

Diferente do protocolo TCP, o UDP não precisa de confirmação no recebimento/envio de suas mensagens. Dessa forma, serviços como jogos on-line, filmes *on demand* e músicas on-line utilizam esse protocolo. Porém, em algumas transmissões, podem ocorrer falhas no envio/recebimento das mensagens, e o protocolo UDP ignora tais erros. Com isso, não pode ocorrer a degradação desses serviços?

Caro estudante, você deve ter percebido que tanto no protocolo TCP quanto no UDP são necessárias portas lógicas para que as mensagens possam ser enviadas pelos protocolos de comunicação, disponíveis na camada de transporte no TCP/IP. Mas, afinal de contas, o que é uma porta lógica?

Ambos os protocolos utilizam as portas lógicas para que ocorra a comunicação com as camadas superiores do protocolo TCP/IP. O número designado para as portas lógicas permite o registro de diversas sessões dos serviços disponíveis nas redes de comunicação de dados.

Os números utilizados pelas portas lógicas estão no intervalo de 0 a 1024, conforme pode ser observado no Quadro 2.4 a seguir:

Quadro 2.4 | Portas lógicas TCP e UDP

PROTOCOLO	SERVIÇO/PROTOCOLO	PORTA
TCP	FTP	21
TCP	Telnet	23
TCP	HTTP	80
TCP/UDP	DNS	53
UDP	FTP	69
UDP	POP3	110
UDP	SMNP	161

Fonte: adaptado de Filippetti (2008, p. 134).

No caso de aplicações que não possuem portas reservadas, é gerado um número aleatório maior ou igual a 1024. As portas acima de 1024 são consideradas "portas altas", por padrão utilizado pelo lado do cliente em uma comunicação. Alguns exemplos podem ser destacados:

- Programas de download via Torrent: normalmente utilizam portas escolhidas aleatoriamente, entre 50000 e 65535.
- IRC (*Internet Relay Chat*): é utilizado para prover serviços de conversação em chats. Normalmente as portas utilizadas nos sockets variam entre 6666 a 6670.

Na camada de rede:

- IP (*Internet Protocol*): protocolo responsável, entre outras coisas, por fornecer o endereçamento para os dispositivos nas redes de computadores. (*Esse protocolo será mais bem descrito na Seção 3.1).
- ICMP (*Internet Control Message Protocol*): tem como objetivo gerenciar os erros no processamento dos datagramas do protocolo IP. Entre eles podem ser destacados:

◊ *Buffer Full*: indica quando um *buffer* atingiu a sua capacidade máxima de processamento.

◊ *Hops*: mostra quantos saltos são necessários para que uma mensagem possa alcançar o seu destino.

◊ *Ping*: mecanismo utilizado para saber se a interface de rede está ativa ou inativa.

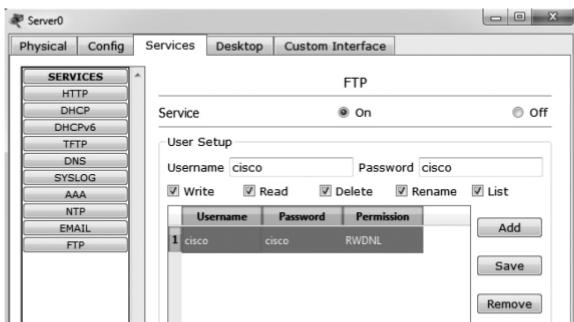
◊ *Traceroute*: esta ferramenta permite mapear os saltos, fornecendo informações como o tempo entre os nodos e o seu respectivo nome.

- ARP (*Address Resolution Protocol*): este protocolo tem a função de permitir conhecer o endereço físico da placa de rede, segundo o seu IP.
- RARP (*Reverse Address Resolution Protocol*): tem função contrária à do ARP, ou seja, deve encontrar o endereço lógico, segundo o endereço físico (placa de rede do dispositivo).

Segundo Forouzan (2008), basicamente as duas principais funções da camada de internet é efetuar o roteamento dos pacotes e fornecer uma interface de rede às camadas superiores (descritas com maiores detalhes na Seção 3.1).

Na camada de rede também é necessário possuir portas lógicas para permitir a comunicação com a camada de transporte.

Pesquise mais

O artigo intitulado *A internet e seu impacto nos processos de recuperação da informação*, de Schiel (2016), demonstra uma aplicação prática do protocolo TCP/IP, em que são demonstradas diversas formas de interação da internet com os principais serviços existentes nas redes de computadores.

Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19651997000100009>. Acesso em: 14 maio 2017.

Sem medo de errar

Os engenheiros da empresa 2@@ estão com dificuldades para efetuar o compartilhamento de arquivos nos projetos para construção de prédios comerciais. Em razão disso, a sua equipe deve configurar o serviço de FTP no servidor encontrado na topologia da empresa.

Para isso, ao clicar em cima do servidor, vá até a opção "*Services*" e, em seguida, FTP. Com isso, é necessário modificar o usuário e a senha já existentes no servidor, em azul conforme demonstrado na Figura 2.17 a seguir:

Figura 2.17 | Usuário FTP

Fonte: elaborada pelo autor.

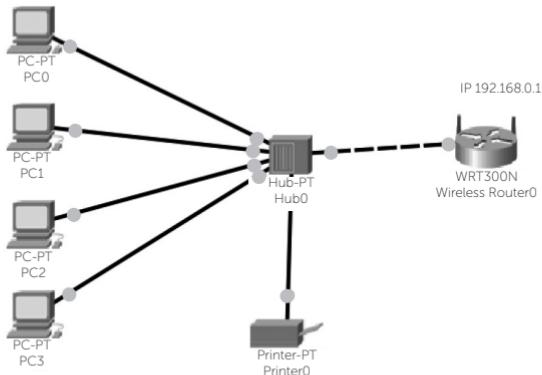
Depois disso, em "*Username*", apague o nome "cisco" e substitua por "Eng"; em "*Password*", apague a senha "cisco", substitua-a por "segredo" e clique em "*Save*" na lateral direita. Repare que, por padrão, todas as autorizações estão habilitadas (*write, read, delete, rename* e *list* – escrever, ler, excluir, renomear e listar) para os arquivos.

Confira o número IP do servidor na aba "Desktop" e após isso em "*IP Configuration*" e anote o número do "*IP Address*", por exemplo 192.168.0.8.

Para efetuar os testes no servidor FTP, escolha um computador na topologia e siga os seguintes passos:

- Clique no computador escolhido, vá na aba "Desktop" e abra o "*command prompt*".
- Para conectar ao servidor FTP digite → ftp número do IP do servidor (Enter no teclado). Ex.: ftp 192.168.0.8. Digite o login do usuário (Eng) e a senha (segredo).
- Para listar os arquivos disponíveis no FTP, digite "dir" e dê enter.
- Para copiar um dos arquivos, digite "get" e o nome do arquivo. Ex.: para copiar o 5º arquivo, deve ser digitado → get c2600-i-mz.122-28.bin
- Para enviar um arquivo para o servidor, devem ser utilizados o "put" e o nome do arquivo. Ex.: put sampleFile.txt. Confira a transferência digitando "dir".
- Observação: para conferir a transferência de arquivo do servidor para o computador, digite "quit" e depois "dir" e confira o nome do arquivo na lista.

Os mesmos testes devem ser repetidos com os computadores localizados na rede da empresa 2@@ .

Ao configurar o servidor para o compartilhamento de arquivos, por meio do protocolo FTP, você pode aplicar uma resolução de problemas enfrentada por diversas companhias com a utilização de protocolos de redes.

Avançando na prática

Rede

Descrição da situação-problema

Uma rede utilizada em um escritório de contabilidade passa por sérios problemas de conflito de endereçamento IP. A sua topologia pode ser observada a seguir:

Figura 2.18 | Topologia do escritório de contabilidade

Fonte: elaborada pelo autor.

Os colaboradores relataram que, antes de perder a conexão com os recursos da rede, surgem algumas mensagens como: "O IP do seu dispositivo foi duplicado na rede" ou "Devido ao conflito de IP, o seu dispositivo não pode mais acessar os recursos da rede".

No contexto apresentado, qual seria uma solução viável para que fossem resolvidos os conflitos de atribuição do endereçamento IP aos dispositivos?

Resolução da situação-problema

Conflitos de atribuição de endereçamento IP nas redes podem ocorrer por falha no DHCP. Na rede em questão, o servidor DHCP é distribuído pelo roteador. Por essa razão, devem ser efetuadas as seguintes alterações:

- O serviço de DHCP deve ser desabilitado no roteador.

- Todos os dispositivos devem ser atribuídos ao IP manualmente, conforme a seguir:
  - ◊ PC0 → IP 192.168.0.2, Máscara de Rede 255.255.255.0, Gateway 192.168.0.1.
  - ◊ PC1 → IP 192.168.0.3, Máscara de Rede 255.255.255.0, Gateway 192.168.0.1.
  - ◊ PC2 → IP 192.168.0.4, Máscara de Rede 255.255.255.0, Gateway 192.168.0.1.
  - ◊ PC3 → IP 192.168.0.5, Máscara de Rede 255.255.255.0, Gateway 192.168.0.1.
  - ◊ Printer0 → IP 192.168.0.6, Máscara de Rede 255.255.255.0, Gateway 192.168.0.1.

Dessa forma, os dispositivos terão IP atribuídos manualmente, evitando assim que os endereços sejam duplicados ou perdidos.

Faça valer a pena

1. Os serviços de *streaming* são utilizados por diversos meios nas redes de computadores, podendo ser providos por empresas que disponibilizam filmes e séries, jogos on-line, sites especializados em vídeos ou música.
Dessa forma, os mecanismos e protocolos utilizados para atender a alta demanda necessitam de profissionais cada vez mais especializados, a fim de garantir o acesso aos serviços com a qualidade desejada.

Os protocolos utilizados para prover a comunicação entre os dispositivos deve permitir que os usuários possam acessar os diversos serviços disponíveis na rede mundial de computadores.
Assinale a alternativa que descreve o protocolo utilizado para prover os serviços do tipo *streaming.*

a) TCP.
b) ICMP.
c) DNS.
d) UDP.
e) DHCP.

2. Um levantamento feito pelo Ibope em 2016 mapeou as preferências dos brasileiros ao acessarem a internet. Em primeiro lugar, está o ato de acessar as redes sociais, seguido por assistir/baixar filmes, ler notícias em portais e escutar músicas. Dos entrevistados, 70% utilizam smartphones para acessar os serviços, entre os quais 93% o fazem por meio da wi-fi em sua residência. (Fonte: Olhar Digital.)
Os serviços mais utilizados se dividem em dois grupos: os de tráfego elástico, ou seja, aqueles que utilizam o protocolo TCP, e os de streaming, que utilizam UDP. Com base nisso, correlacione entre si as duas colunas a seguir:

Protocolo	Característica
(T) Protocolo TCP	( ) Comunicação sequencial
(U) Protocolo UDP	( ) Comunicação confiável
	( ) Baixa latência
	( ) Comunicação orientada à conexão
	( ) Sem retransmissão de pacotes perdidos.

Assinale a alternativa com a sequência correta de correlação, de cima para baixo:
a) T – U – U – T – T.
b) T – U – T – U – T.
c) U – T – U – T – U.
d) T – T – U – T – U.
e) U – U – T – U – U.

3. Em 1938, Orson Welles anunciou, por uma rádio de Nova York, que os alienígenas estariam invadindo os Estados Unidos. A notícia se espalhou de maneira estrondosa, causando pânico na população e tumulto nos supermercados e nas delegacias de vários estados. Os estragos poderiam ter sido maiores se houvesse um meio de comunicação como os encontrados atualmente.

As redes de dados atualmente possibilitam diversas aplicações que trouxeram comodidade e praticidade aos usuários. Para que os serviços possam ser utilizados, são necessários protocolos de comunicação para o seu funcionamento.
O diagrama a seguir representa as camadas do protocolo TCP/IP em relação ao modelo de referência OSI.

OSI		TCP/IP
Aplicação		
Apresentação		________
Seção		
Transporte		________
Rede		________
Enlace		________
Física		

Assinale a alternativa com a sequência de termos que completem corretamente o nome de cada uma das camadas (da camada superior para a inferior):

a) Apresentação – internet – transporte – enlace.
b) Aplicação – sessão – transporte – rede.
c) Apresentação – aplicação – transporte – internet.
d) Aplicação – sessão – transporte – enlace.
e) Aplicação – transporte – internet – acesso à rede.

Referências

FILIPPETTI, M. A. **Guia completo de estudos**. CCNA 4.1 Florianópolis: Visual Books, 2008.

FOROUZAN, A. **Comunicação de dados e redes de computadores**. São Paulo: McGraw, 2008.

KUROSE, J. F. **Redes de computadores e a internet:** Uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

STEVENS, R. W. **TCP/IP Illustrated**. v. 1: *The Protocols.* Boston: Addison-Wesley, 1994.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 1997.

Arquitetura e tecnologias de redes

Convite ao estudo

Caro aluno, conforme avançamos nos estudos acerca de redes de computadores, é necessário compreender mais técnicas, para que possamos planejar, implementar e gerenciar: infraestrutura física e lógica, serviços e aplicações.

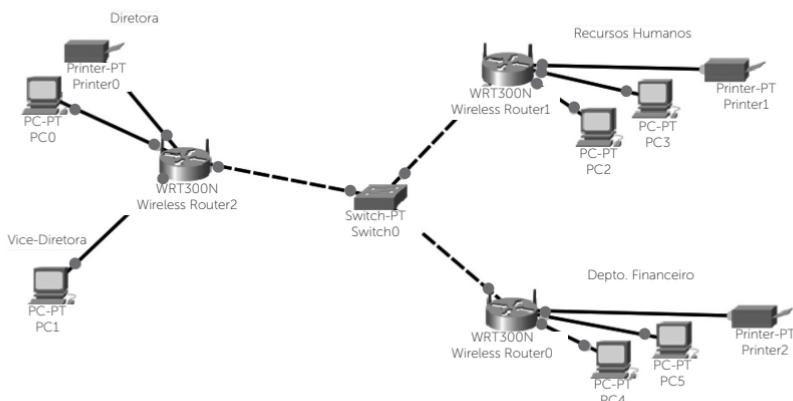
Para isso, na Seção 3.1 você utilizará as técnicas de endereçamento IP (*Internet Protocol*) para planejar a atribuição de endereçamento nos dispositivos, possibilitando, assim, o planejamento de sub-redes em qualquer topologia. Esses estudos permitirão que você planeje como uma rede pode ser segmentada, para isolar departamentos, por meio de técnicas de manipulação do endereço IP.

Na Seção 3.2, serão discutidos conceitos e características relacionados à ethernet, seu modo de operação, domínio de colisão e broadcast. Com isso, você compreenderá alguns parâmetros de performance das redes e a função do domínio de colisão e de broadcast (necessidade e consequências).

Finalmente, na Seção 3.3, serão apresentadas as diferenças entre as duas versões do protocolo IP: o IPv4 e IPv6. Isso revelará a necessidade de técnicas que permitem a coexistência e a interoperabilidade entre os protocolos na mesma rede. Tais conhecimentos possibilitarão planejar redes com as duas versões do IP e efetuar uma reflexão sobre o futuro das redes de computadores.

Com as técnicas estudadas nesta unidade, você poderá se tornar um profissional com a capacidade de desenvolver um planejamento da infraestrutura lógica de uma rede de comunicação, com diversos serviços e dispositivos.

Você está pronto para mais esse desafio? Então vamos em frente.

Seção 3.1

Redes e sub-redes

Diálogo aberto

O projeto desenvolvido na empresa 2@@ (na Unidade 2) fez com que a sua equipe ganhasse mais confiança das empresas. Os bons serviços prestados refletiram em mais uma indicação. A Escola 1_A é uma instituição de ensino que atende alunos do ensino fundamental II e do ensino médio. A sua estrutura física possui laboratórios de informática, laboratório de Física/Química, quadras para práticas esportivas e uma grande biblioteca.

Nas últimas semanas, os departamentos administrativos (direção, recursos humanos e financeiro) vêm enfrentando algumas dificuldades em sua rede. A topologia apresentada na Figura 3.1 demonstra a infraestrutura física da escola:

Figura 3.1 | Topologia da escola Escola 1_A

Fonte: elaborada pelo autor.

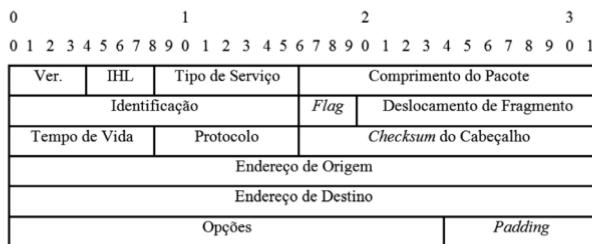
Em um diagnóstico primário, a sua equipe percebeu que está ocorrendo algum problema de conflito de endereçamento IP. Para solucionar isso, foi proposto segmentar a rede em cinco sub-redes, separando direção da escola, recursos humanos, departamento financeiro, marketing e acadêmico.

Para isso, você deve fazer um relatório que contenha uma tabela com o endereço de rede, a faixa de IP válidos e o endereço de

broadcast de cada uma das sub-redes. A classe utilizada quando a rede foi desenvolvida foi 192.168.20.0 e máscara 255.255.255.0.

O desenvolvimento da tabela de sub-redes permitirá que você compreenda as técnicas para planejamento por meio da divisão das redes de computadores em quantas sub-redes forem necessárias.

Vamos resolver mais esse problema?

Não pode faltar

Caro aluno, desde o início dos estudos relacionados à rede de computadores, foi mencionado e aplicado o endereçamento nos dispositivos, como: computadores, impressoras e nodos de rede (aquele número do tipo 192.168.0.50). Tais configurações foram feitas por você de forma intuitiva, pois até este momento não foi abordado um dos mais importantes tópicos: o endereçamento IP e as suas técnicas de sub-redes.

Nesta seção será abordada somente a versão 4 do protocolo, ou seja, o IPv4. O IPv6, versão mais recente do endereçamento, será tratado na Seção 3.3.

Segundo Kurose (2006), o *Internet Protocol*, ou simplesmente IP, é o endereço lógico feito para que um dispositivo possa se comunicar com qualquer outro dispositivo, independentemente de sua localização geográfica.

Conforme determina a RFC 791 (para a versão 4), o IP possui 32 bits, sendo possível produzir 2^{32} = 4,3 bilhões de endereços.[1] O protocolo está definido na camada de rede, sendo o seu pacote denominado datagrama, cujos campos podem ser observados na Figura 3.2:

Figura 3.2 | Formato do Datagrama IPv4

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Ver.	IHL	Tipo de Serviço	Comprimento do Pacote	
Identificação			*Flag*	Deslocamento de Fragmento
Tempo de Vida		Protocolo	*Checksum* do Cabeçalho	
Endereço de Origem				
Endereço de Destino				
Opções				*Padding*

Fonte: Kurose (2006, p. 256).

[1] RFC 791. Disponível em: <https://tools.ietf.org/html/rfc791>. Acesso em: 16 jun. 2017.

Onde:

Versão: campo que traz a versão do protocolo IP (4 ou 6).

IHL: determina o tamanho do cabeçalho.

Tipo de serviço: determina a prioridade do pacote.

Comprimento do pacote: fornece o tamanho total do pacote, incluindo o cabeçalho e os dados.

Identificação: identifica o fragmento do pacote IP original.

Flag: é dividido em Flag mais Fragmentos (MF), usado para o deslocamento dos datagramas e, posteriormente, a sua reconstrução, e em Flag não Fragmentar (DF), que indica que a fragmentação do pacote não é autorizada.

Deslocamento de fragmento: responsável por identificar a ordem dos pacotes no processo de remontagem.

Tempo de vida: identificado como TLL (*time to live*), indica o "tempo de vida" que o pacote possui a cada salto pelos nós.

Protocolo: responsável por repassar os dados para os protocolos corretos que estão nas camadas superiores.

Checksum do cabeçalho: responsável por informar os erros no cabeçalho.

Endereço de origem: identifica o endereço do remetente.

Endereço de destino: identifica o endereço do receptor.

Opções: implementações opcionais.

Padding: preenchimento.

Caro aluno, para a compreensão do formato do endereçamento IP, faremos uma analogia com os números utilizados em telefonia fixa.

55 19 3517-1234

55 → Identifica o número do país.

19 → Classifica uma região com vários municípios.

3517 → Determina uma central telefônica.

1234 → Número do assinante.

Seguindo essa lógica, a notação de um endereço IP é separada por ponto, fazendo com que uma parte identifique a rede e a outra, o dispositivo (*host*). Por exemplo:

172.16.30.110

172.16 → identifica à qual rede o dispositivo pertence.

30.110 → determina o endereço do dispositivo.

Segundo Kurose (2006), os endereçamentos utilizados nas redes foram divididos em classes para utilização de acordo com o número de dispositivos da rede, conforme é possível observar no Quadro 3.1 a seguir:

Quadro 3.1 | Classes de Endereço IP

	8 bits	8 bits	8 bits	8 bits	Intervalo
Classe A	NET	HOST	HOST	HOST	0 – 127
Classe B	NET	NET	HOST	HOST	128 – 191
Classe C	NET	NET	NET	HOST	192 – 223
Classe D	Classe reservada para endereços de multicast				
Classe E	Classe reservada para pesquisa				

Fonte: Filippetti (2008, p. 147).

Caro aluno, para que fique mais clara a compreensão do Quadro 3.1, observe os exemplos de cada uma das classes:

- Classe A: 10.0.0.50, em que 10 é o endereço de rede e 0.0.50 é o endereço de host.
- Classe B: 172.16.31.10, em que 172.16 é o endereço de rede e 31.10 é o endereço de host.
- Classe A: 192.168.0.20, em que 192.168.0 é o endereço de rede e .20 é o endereço de host.

Além da divisão por classes, a utilização deve obedecer:

- IP para rede privada: números de IP reservados para utilização dentro das LANs, sendo usados os seguintes endereçamentos nos seguintes intervalos:

◊ Classe A: 10.0.0.0 a 10.255.255.255

◊ Classe B: 172.16.0.0 a 172.31.255.255

◊ Classe C: 192.168.0.0 a 192.168.255.255

- IP para rede pública: faixas de números de IP utilizados para dispositivos acessíveis pela internet. Por exemplo, os servidores como o 201.55.233.117 (endereço do site google.com.br).

Os números naturais N={0, 1, 2, 3, 4, 5, ...} são inteiros e positivos (incluindo o zero). A ordem dos números IP se inicia no 0 e é finalizada no 255. Dessa forma,- poderíamos ter:

192.168.0.0 → 192.168.0.1 → 192.168.0.2 → ... → 192.168.0.255

Caro aluno, sempre que vamos configurar os IPs dos dispositivos de uma rede, são necessárias algumas configurações. Observe a Figura 3.3 a seguir:

Figura 3.3 | Configuração de número IP

```
Endereço IPv4. . . . . . . .  . . . . . . . . : 192.168.0.101
Máscara de Sub-rede . . . . . . . . . . . . . : 255.255.255.0
Gateway Padrão. . . . . . . . . . . . . . . . : 192.168.0.1
```

Fonte: elaborada pelo autor.

Você deve ter percebido que, além do IP (192.168.0.101), existem outros números importantes para conseguir acessar os recursos, entre os quais estão:

Gateway (visto na Seção 1.3), a saída das mensagens na rede interna. Normalmente é o IP do equipamento (roteador ou *switch*) na borda da rede interna. No exemplo da Figura 3.3, é o IP 192.168.0.1.

Máscara de sub-rede é a técnica utilizada para definir qual porção do número IP é designada para identificar o host e a rede (network). No exemplo da Figura 3.3, é o IP 255.255.255.0.

Segundo Filippetti (2008), a máscara de rede possui 32 bits, possuindo padrão para as classes A, B e C, conforme pode ser observado no Quadro 3.2:

Quadro 3.2 | Máscara padrão

Classe	Formato	Máscara padrão
A	Rede.Host.Host.Host	255.0.0.0
B	Rede.Rede.Host.Host	255.255.0.0
C	Rede.Rede.Rede.Host	255.255.255.0

Fonte: Filippetti (2008, p. 153).

Caro aluno, agora que você compreendeu o formato do IP e da máscara, é necessário entender como são formados os octetos, que são os números separados por ponto.

Para isso, lembre-se de que a contagem dos números IP vai de *0* a *255*, podendo se representar pelos valores: 128, 64, 32, 16, 8, 4, 2, e 1. Se efetuarmos a soma desses valores, teremos *255*, ou seja, é possível representar qualquer endereço de rede binariamente, no intervalo de 0 a 255.

Para efetuar a conversão, é necessário fazer a somatória dos bits ligados, dos valores no qual se deseja representar. Observe o exemplo a seguir, em que o endereço 192.168.0.22 foi convertido em binário:

Quadro 3.3 | Conversão para binário

	128	64	32	16	8	4	2	1
192	1	1	0	0	0	0	0	0
168	1	0	1	0	1	0	0	0
0	0	0	0	0	0	0	0	0
22	0	0	0	1	0	1	1	0

Fonte: Filippetti (2008, p. 153).

No primeiro octeto foram ligados apenas os números 128 e 64, resultando em 192, que é a primeira parte do endereço IP. Portanto, é possível representar todos os endereços utilizados nas redes de computadores baseadas em IPv4. Dessa forma, o endereço IP 192.168.0.22 pode ser representado em binário como: 11000000. 10101000.00000000.00010110.

Reflita

As máscaras de sub-redes são utilizadas em conjunto do IP para a definição das funções de cada octeto no endereçamento de um dispositivo. Mas, se fosse necessário fazer a conversão das máscaras padrão para binário, como ficariam os seus formatos?

Caro aluno, compreender a conversão de endereço IP para binário vai auxiliá-lo no cálculo de sub-redes. Mas, afinal, o que é sub-rede?

Segundo Tanenbaum (1997), também conhecida como *subnet*, essa técnica permite a segmentação de uma rede em diversas sub-redes, que podem ser isoladas das demais ou não. Isso permite que o administrador dentro de uma faixa de IP possa ter:

- Redução do tráfego de rede, pois os nodos dentro das sub-redes fazem domínio de broadcast, mensagens enviadas para todos os nodos da rede.
- Simplificação no gerenciamento da rede, pois facilita-se a identificação de falhas pelo mapeamento do endereço da sub-rede.
- Controle dos recursos da rede, pois possibilita-se "enxergar" uma grande rede, como diversas LANs isoladas.

Em diversas empresas, é necessário dividir alguns setores em: financeiro, recursos humanos, tecnologia da informação, entre outros. As motivações podem estar ligadas à segurança, ao controle ou ao gerenciamento.

O intuito de desenvolver redes em sub-redes pode estar na necessidade de alocação de mais recursos, para garantir que os serviços prioritários fiquem disponíveis. Exemplo: isolar em uma sub-rede uma impressora utilizada por todos os departamentos permite que o usuário não enfrente filas de impressão, aumentando, assim, a disponibilidade do recurso na rede.

Para calcular as sub-redes, vamos tomar de exemplo uma rede de classe C, em que a faixa de IP utilizada deve ser 192.168.0.0; e a máscara padrão, 255.255.255.0, sendo desejado fazer quatro sub-redes. Para isso, Filippetti (2008) define que:

1º passo: faça a conversão da máscara de rede para binário:

255.255.255.0 → 11111111.11111111.11111111.00000000

2º passo: efetue o cálculo da quantidade de hosts possível em cada uma das sub-redes, em que "n" é o número de bits necessário para determinar:

- Rede: $2^n = 2^2 = 4$, ou seja, para fazer quatro sub-redes, será necessário "tomar emprestados" dois bis da máscara de rede.
- Hosts por sub-rede: $2^n = 2^6 = 64$, ou seja, cada sub-rede poderá utilizar 64 endereços.

Você deve estar se perguntando: por que 2^6? De onde surgiu o 6?

Lembre-se de que para converter os octetos, são utilizados: 128, 64, 32, 16, 8, 4, 2, 1; portanto, se, para determinar o número de redes, foram emprestados 2 bits, então sobraram 6 bits para determinar o número de hosts.

3º passo: construa a tabela de sub-redes:

Vale aqui ressaltar que, dentro da faixa de uma sub-rede, o primeiro endereço não deve ser utilizado, pois é reservado para identificação da rede, e o último é utilizado para Broadcast.

Rede	1º IP Válido	Ultimo IP Válido	Broadcast
192.168.0.0	192.168.0.1	192.168.0.62	192.168.0.63
192.168.0.64	192.168.0.65	192.168.0.126	192.168.0.127
192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
192.168.0.192	192.168.0.193	192.168.0.254	192.168.0.255

Nesse exemplo, repare na primeira linha: o endereço de rede atribuído foi 192.168.0.0; já na segunda rede foi utilizado o 192.168.0.64. Dessa forma, o endereço de Broadcast da primeira rede tem que ser um anterior ao endereço de rede da segunda linha, isto é, 192.168.0.63. Os IPs válidos, ou seja, os que podem ser utilizados nos dispositivos, estão entre o intervalo dos endereços de Rede e de Broadcast.

4º passo: determinar a nova máscara de rede:

Para determinar o número de rede, foi necessário "tomar emprestados" dois bits da máscara. Dessa forma, se a máscara padrão convertida no passo 1 foi 11111111.11111111.11111111.000000 00, ao tomarmos emprestados 2 bits, temos que:

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Com a soma dos bits ligados, teremos 128 + 64 = 192.

Portanto, na nova máscara de sub-rede que vai permitir segmentar a rede em quatro partes, deve ser utilizado o número 255.255.255.192.

Em binários poderíamos representá-lo por: 11111111.11111111.11111111.11000000 (contando-se os bits ligados, tem-se 26 bits). Com base nessa representação, é possível expressar um endereço e a sua respectiva máscara, por exemplo: 192.168.0.1/26. Ou seja, são representados o endereço IP 192.168.0.1 utilizado para identificar um dispositivo e a sua respectiva máscara de rede 255.255.255.192.

Para utilizar essa técnica para desenvolvimento de sub-redes nas classes A e B, deve-se seguir o mesmo conceito apresentado para a classe C.

Endereço de broadcast

Quando foi desenvolvida a tabela com as sub-redes, você deve ter percebido que o último endereço é reservado para mensagens do tipo broadcast (última coluna). Commer (2007) indica a difusão de um pacote para todos os dispositivos da rede (se o contexto for de uma sub-rede, então somente aos dispositivos desta). Ao receber a mensagem, o dispositivo deve "ler" o pacote e verificar se lhe pertence. Se pertencer a ele, a mensagem é respondida, caso contrário o pacote é descartado.

Veja um exemplo: ao ligarmos um computador em uma rede, este emite uma mensagem de broadcast solicitando um endereço IP ao servidor DHCP. Os computadores e demais dispositivos descartam a solicitação e, então, o servidor DHCP responde ao pedido, atribuindo um endereço ao computador ligado.

Endereço de *loopback* (127.0.0.1)

Trata-se de um endereço reservado para teste de comunicação nos processos ocorridos na interface de rede do próprio dispositivo. Por padrão, os profissionais de redes e programadores utilizam o endereço 127.0.0.1, conforme é possível observar na Figura 3.4:

Figura 3.4 | Teste *loopback*

```
C:\Users\Prof. Serginho Nunes>ping 127.0.0.1

Disparando 127.0.0.1 com 32 bytes de dados:
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 127.0.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 0ms, Média = 0ms
```

Fonte: elaborada pelo autor.

Com base na Figura 3.4, é possível confirmar o funcionamento da interface de rede e o protocolo TCP/IP quando são enviados quatro pacotes com todos recebidos, dentro do tempo (1 ms).

Além da aplicação do IP na telefonia, tecnologia conhecida como VoIP, é possível utilizar o protocolo IP para transmissão de TVoIP. O intuito dessa tecnologia é prover a distribuição de serviços televisivos sob demanda, em que se utiliza a transmissão sobre o protocolo IP (conhecido também como IPTV).

Para saber mais, leia o artigo intitulado "TVoIP: TV sobre IP Arquiteturas para Transmissão em Larga Escala", disponível em: <http://www2.ic.uff.br/~celio/papers/minicurso-sbrc06.pdf> (acesso em: 3 jun. 2017).

Caro aluno, a partir das definições vistas até aqui, é possível compreender os mecanismos de roteamento. Tanenbaum (1997) define que o roteamento é a técnica utilizada para encaminhar as mensagens através das redes. Os processos envolvidos devem:

- Determinar os caminhos possíveis da origem até o destino.
- Selecionar o melhor caminho.
- Identificar se o pacote pertence a uma sub-rede e garantir que ele alcance o seu destino.

Dessa forma, equipamentos como os roteadores (os *switches* gerenciáveis também) podem consultar a sua tabela de roteamento e, por meio do endereçamento disponível no cabeçalho TCP/IP, efetuar o encaminhamento correto das mensagens.

Sem medo de errar

A escola Escola 1_A é uma instituição de ensino fundamental II e ensino médio. Possui uma infraestrutura completa para atender os seus alunos com excelência.

A rede interna da escola vem enfrentando algumas dificuldades, pois ocorrem muitas falhas e lentidões. Para isso, foi proposto segmentar a rede em cinco sub-redes (direção, recursos humanos, departamento financeiro, marketing e acadêmico), na rede 192.168.20.0 e máscara 255.255.255.0.

Para isso, é necessário desenvolver uma tabela contendo o endereço de rede e a faixa de IP válidos, além do endereço de broadcast de cada uma das sub-redes. Veja o desenvolvimento proposto:

Máscara em binário: 255.255.255.0 → 11111111.11111111.11111111.00000000

Quantidade de redes $= 2^n = 2^3 = 8$ redes.

Quantidade de *hosts* por sub-rede $= 2^n = 2^5 = 32$ hosts.

Rede	Faixa de IP Válido	Broadcast
192.168.0.0	192.168.0.1 a 192.168.0.30	192.168.0.31
192.168.0.32	192.168.0.33 a 192.168.0.62	192.168.0.63
192.168.0.64	192.168.0.65 a 192.168.0.94	192.168.0.95
192.168.0.96	192.168.0.97 a 192.168.0.126	192.168.0.127
192.168.0.128	192.168.0.129 a 192.168.0.159	192.168.0.160

Binário da nova máscara de rede: 11111111.11111111.11111111.11100000

128 64 32 16 8 4 2 1

1 1 1 0 0 0 0 0, ou seja, 224 bits ligados.

Nova máscara = 255.255.255.224 ou /27.

Repare ainda que é possível desenvolver mais três sub-redes, pois, como a quantidade de sub-redes é sempre múltiplo de 2 e a necessidade era criar 5 sub-redes, para atender à demanda foram feitas $= 2^3 = 8$ sub-redes.

Avançando na prática

Rede Cidade Universitária

Descrição da situação-problema

Uma cidade universitária é um *campus* com diversos departamentos. A Figura 3.5 representa a vista aérea do Campus Butantã da USP/SP.

Figura 3.5 | Vista Aérea USP

Fonte: <https://goo.gl/T8zy5x>. Acesso em: 4 jun. 2017.

Nesse contexto, você foi contratado para efetuar as manutenções diárias nas 10 sub-redes do *campus*. Ao iniciar o seu turno, o software de monitoramento da rede acusou que o quinto endereço utilizável da terceira sub-rede 172.16.0.0 está com problemas na interface de rede. Qual é o IP do dispositivo em questão?

Resolução da situação-problema

Máscara padrão: 255.255.0.0

Representação binária: 11111111.11111111.00000000.00000000

Quantidade de redes = $= 2^n = 2^4 = 16$ redes

Quadro 3.4 |

Rede	Faixa de IP Válido	Broadcast
172.16.0.0	172.16.0.1 a 172.16.15.254	172.16.15.255
172.16.16.0	172.16.16.1 a 172.16.31.254	172.16.31.255
172.16.32.0	172.16.32.1 a 172.16.47.254	172.16.47.255

Como o intervalo de IPs válidos da terceira sub-redes é 172.16.32.1 a 172.16.47.254. Dessa forma:

1° IP válido: 172.16.32.1

2° IP válido: 172.16.32.2

3° IP válido: 172.16.32.3

4° IP válido: 172.16.32.4

5° IP válido: 172.16.32.5

Ou seja, o endereço do dispositivo que apresenta problemas é o 172.16.32.5.

Faça valer a pena

1. As redes de comunicação estão presentes em mais de 50% dos lares brasileiros e na grande maioria das empresas e comércios. A necessidade de ter uma estrutura de rede com impressoras, computadores e servidores fez com que o profissional de redes fosse necessário para garantir a qualidade dos serviços.
Conhecer os aspectos técnicos/conceituais a respeito dos endereços utilizados nas infraestruturas pode representar um diferencial
Com base nesse contexto, observe as afirmativas a seguir:

I. As faixas de IP são divididas em seis classes: A, B, C, D, E e F.
II. A máscara é um endereço que independe do IP, cada um tem funções distintas nas redes.
III. O endereço 255.255.0.10 pode ser representado em binário como 1111 1111.11111111.00000000.00001010
Assinale a alternativa correta:
a) Somente as afirmativas I e III são verdadeiras.
b) Somente a afirmativa III é verdadeira.
c) Somente as afirmativas I e II são verdadeiras.
d) Somente as afirmativas II e III são verdadeiras.
e) Somente a afirmativa II é verdadeira.

2. Em diversas situações, o administrador de redes necessita dividir a sua rede em diversas sub-redes, a fim de isolar os departamentos para garantia de integridade, gerenciamento centralizado dos recursos, entre outras necessidades.
Para isso, os administradores de redes utilizam as técnicas como o cálculo de sub-redes por meio da manipulação da máscara de rede.

Para utilizar as técnicas de sub-redes, por meio da alteração da máscara de sub-redes, é necessário conhecer a máscara padrão utilizada. Observe Quadro 3.5 a seguir:

Quadro 3.5 | Classes de sub-redes

Classe	Máscara padrão
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Fonte: elaborado pelo autor.

Assinale a alternativa que represente corretamente a porção destinada à rede e aos *hosts* da classe B:

a) Rede.Rede.Rede.Rede
b) Rede.Rede.Rede.Host
c) Host.Host.Host.Host
d) Rede.Host.Host.Host
e) Rede.Rede.Host.Host

3. Segmentar uma rede pode trazer: redução do tráfego de rede, pois os nodos dentro das sub-redes fazem domínio de broadcast; simplificação no gerenciamento da rede, pois facilita a identificação de falhas pelo mapeamento do endereço da sub-rede; controle dos recursos da rede, pois possibilita "enxergar" uma grande rede, como diversas LANs isoladas.

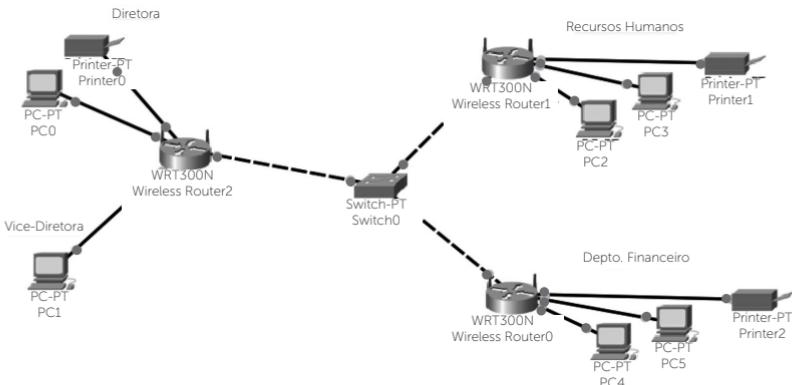
Como primeiro passo, a máscara de rede deve ser convertida em binário. Observe as afirmativas a seguir e indique (V) para as verdadeiras ou (F) para as falsas:

( ) A máscara 255.255.0.255 em binário é 11111111.11111111.00000000.11111111
( ) O binário 11111111.01100000.00000000.00000000 no formato de endereço de rede é 255.128.0.0
( ) A máscara 255.255.255.20 em binário é 11111111.11111111.11111111.11000000
( ) O binário 11111111.00000000.00000000.00000000 no formato de endereço de rede é 255.0.0.0
( ) A máscara 255.255.255.96 em binário é 11111111.11111111.11111111.01100000

Assinale a alternativa com a sequência correta de indicações, de cima para baixo:

a) F – V – V – F – F.
b) V – F – V – F – V.
c) V – F – F – V – V.
d) F – V – F – V – F.
e) F – F – F – V – F.

Seção 3.2

Ethernet

Diálogo aberto

No projeto da escola Escola 1_A, a sua equipe realizou um excelente trabalho ao criar sub-redes separando os departamentos. Tais alterações na rede foram sentidas pelos colaboradores no ganho de velocidade no acesso aos recursos e nos compartilhamentos. Fora esses apontamentos feitos pelos usuários, a rede ganhou em segurança ao isolar as informações de setores distintos.

Para que seja criado um histórico das redes desenvolvidas pela sua equipe, o diretor de projetos solicitou que fossem documentados os equipamentos contidos em cada um dos departamentos e a quantidade de domínios de colisão e de broadcast na rede da unidade escolar.

Para isso, observe a Figura 3.1 em que está representada a topologia da escola Escola 1_A, possibilitando listar os equipamentos por departamento (direção, RH e financeiro) e calcular os domínios de colisão e broadcast.

Figura 3.1 | Topologia da escola Escola 1_A

Fonte: elaborada pelo autor.

A compreensão dos domínios de colisão e broadcast auxiliará você no planejamento para estruturação de uma rede, sendo possível

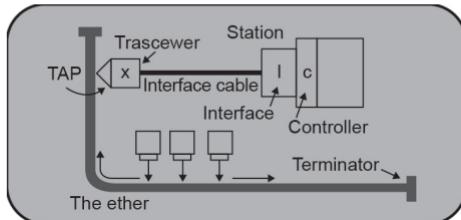
escolher o equipamento apropriado para que a rede tenha o melhor desempenho possível. Para isso, faça, em forma de relatório, o levantamento solicitado pelo diretor de projetos.

Não pode faltar

Caro aluno, se imaginarmos a rede mundial de computadores, vamos perceber que a maior parte das topologias se encontra em uma LAN, onde estão localizadas as redes residenciais, empresas, faculdades, comércio, entre outros locais. Nesta seção você vai poder compreender as tecnologias utilizadas nas redes Ethernet, os domínios de colisão e broadcast, conhecimentos esses que possibilitarão que você consiga planejar a estrutura de uma rede interna com a garantia de qualidade nos serviços disponíveis.

Segundo Tanenbaum (1997), pode se definir Ethernet como um padrão utilizado em transmissões em redes locais (Norma IEEE 802.3). As normas IEEE 802 possuem subgrupos, conforme ilustra o Quadro 3.6:

Quadro 3.6 | Subgrupos 802

Subgrupo	Definição
IEEE 802.1	Gerência de rede
IEEE 802.2	*Logical link control*
IEEE 802.3	Ethernet
IEEE 802.5	*Token ring*
IEEE 802.6	Redes metropolitanas
IEEE 802.7	Rede metropolitana
IEEE 802.8	Fibra óptica
IEEE 802.10	Segurança em rede local
IEEE 802.11	Rede sem fio (Wireless)
IEEE 802.15	Rede PAN (bluetooth)
IEEE 802.16	Rede Wi-Max

Fonte: adaptado de Tanenbaum (1997, p. 254).

Especificamente nesta seção será feita uma discussão aprofundada sobre a Norma 802.3, que define as características técnicas e demais assuntos relacionados às redes locais (Ethernet). Basicamente, esse tipo de rede deve ter dois pontos:

- Conexão dos dispositivos: devem estar conectados em uma mesma linha de comunicação.
- Meios de ligação: devem ser constituídas por cabos cilíndricos (visto em detalhes no Quadro 3.7 à frente).

Inicialmente, a Ethernet foi descrita por Robert Metcalfe (1973) em um projeto desenvolvido na empresa Xerox, conforme pode ser observado na Figura 3.6:

Figura 3.6 | Esquema 802.3

Fonte: <https://goo.gl/NbWGz5>. Acesso em: 10 jun. 2017.

Por volta de 1979, Robert Metcalfe deixou a Xerox para criar a 3Com, empresa esta que, embora possua equipamentos até hoje nas redes, teve as suas atividades encerradas no ano de 2010. A grande sacada do seu fundador foi conseguir convencer as empresas DEC, Intel e Xerox a firmar parceria para conseguir estabelecer a Ethernet como um padrão utilizado nas redes de computadores local.

Caro aluno, embora na Unidade 1 nós tenhamos estudado alguns meios de transmissão, para auxiliar a compreensão das características das redes Ethernet, vale a pena observar alguns exemplos de diferentes tipos de cabeamentos utilizados nas redes IEEE 802.3:

Quadro 3.7 | Subgrupos 802

Sigla	Característica	Cabo	Conector	Débito	Distância
10Base2	Ethernet fina	Cabo coaxial (50 Ohms) de diâmetro fino	BNC	10 Mb/s	185 m
10Base5	Ethernet espessa	Cabo coaxial de diâmetro espesso	BNC	10Mb/s	500 m
10Base-T	Ethernet padrão	Par trançado (categoria 3)	RJ-45	10 Mb/s	100 m
100Base-TX	Ethernet rápida	Duplo par trançado (categoria 5)	RJ-45	100 Mb/s	100 m

CAT6	Ethernet Gigabit	Duplo par trançado (categoria 6)	RJ-45	1000 Mbit/s	550 m
CAT6a	Ethernet de 10 Gigabits	Duplo par trançado (categoria 6)	RJ-45	10 Gbit/s	550 m
100Base-FX	Ethernet rápida	Fibra óptica multimodo (tipo 62.5/125)	****	100 Mb/s	2 km
1000Base-T	Ethernet Gigabit	Duplo par trançado (categoria 5)	RJ-45	1000 Mb/s	100 m
1000Base-LX	Ethernet Gigabit	Fibra óptica monomodo ou multímodo	****	1000 Mb/s	550 m
1000Base-SX	Ethernet Gigabit	Fibra ótica multímodo	****	1000 Mbit/s	550 m
10GBase-SR	Ethernet de 10 Gigabits	Fibra ótica multímodo	****	10 Gbit/s	500 m
10GBase-LX4	Ethernet de 10 Gigabits	Fibra ótica multímodo	****	10 Gbit/s	500 m

Fonte: Filippetti (2008, p. 57).

Exemplificando

Nas transmissões em que é possível alcançar velocidades de 1 Gbps, é utilizado cabeamento do tipo CAT6. Por sua vez, em transmissões com velocidades com até 10 Gbps, utiliza-se o CAT6a.

A seguir é possível observar a diferença entre os cabos do tipo CAT5e e CAT6:

Figura 3.7 | CAT5e *versus* CAT6

Fonte: <https://goo.gl/1dPzyy>. Acesso em: 10 jun. 2017.

Os cabeamentos utilizados na tecnologia Ethernet possuem valores mais acessíveis do que aqueles utilizados em uma WAN, por exemplo. Segundo Filippetti (2008), o tipo de tecnologia aplicada ao cabeamento dita a velocidade que cada um deles pode atingir, sendo estas as mais utilizadas nas aplicações IEEE 802.3:

- Fast Ethernet (Ethernet rápida): definida como IEEE 802.3u, permitiu que a velocidade de transmissão atingisse 100 megabits, sendo encontrada como: 100Base-TX, 100Base-T e 100Base-FX.
- Ethernet Gigabit: dez vezes superior à Fast Ethernet, versão que permite velocidades de transmissão de até 1.000 megabits. O padrão foi definido como 802.3z. Possibilitam-se quatro tipos: 1000BASE-LX, 1000BASE-SX, 1000BASE-CX e 1000BASE-T.
- Ethernet 10 Gigabit: da mesma forma como ocorreu na versão anterior, este padrão multiplicou a sua capacidade em 10 vezes, permitindo atingir uma velocidade de 10 Gigabit Ethernet, sendo também conhecido como 10G. Entre as opções estão as tecnologias: 10GBASE-LR, 10GBASE-ER, 10GBASE-ZR, 10GBASE-SR, 10GBASE-LRM e 10GBASE-CX4.

Métodos de transmissão Ethernet

Na Seção 3.1, você estudou diversos protocolos de rede que podem ser utilizados nas redes WAN e/ou LAN. Porém, em relação às redes Ethernet, Tanenbaum (1997) aponta que as comunicações desse tipo de rede são efetuadas pelo protocolo CSMA/CD (*carrier sense multiple access with collision detection*), que permite que qualquer dispositivo da rede possa efetuar uma transmissão sem hierarquizar quem tem prioridade.

Basicamente, para o funcionamento do protocolo os dispositivos verificam se não há nenhuma comunicação ocorrendo para assim fazer uma transmissão. Caso ocorra de dois dispositivos emitirem uma mensagem um para o outro simultaneamente, ocorre uma colisão (mais à frente será abordado o assunto "colisão" com mais detalhes), e a transmissão é interrompida, sendo retomada em um tempo aleatório.

Caro aluno, para a melhor compreensão dessa técnica, vamos compreender o que significam as suas siglas:

- CSMA (*carrier sense multiple access* – acesso múltiplo com detecção de portadora): trata-se de um protocolo que faz a transmissão com base na detecção da existência de uma transmissão, com o qual é possível utilizar três algoritmos:

◊ CSMA não persistente: se o meio de transmissão estiver ocupado, o dispositivo espera um tempo aleatório e tenta retransmitir até conseguir.

◊ CSMA 1 persistente: o dispositivo "escuta" a rede até que o meio fique livre e, então, procede com a transmissão.

◊ CSMA p-persistente: o algoritmo calcula a probabilidade de colisão e, quando livre e com baixa ou nenhuma possibilidade de colisão, procede com a transmissão.

- CD (*coilision detection* – detecção de colisão): o mecanismo CD faz com que os nodos existentes na rede "escutem" a rede e possam detectar colisões (técnica conhecida como LTW – *listen while talk* – escuta enquanto fala). Quando é detectada uma colisão, o nodo emite um pacote alertando todos os dispositivos.

Filippetti (2008) define que as transmissões 802.3 utilizam um cabeçalho de 14 bytes, dos quais:

- 6 bytes: são utilizados para o endereço de origem.
- 6 bytes: são para o endereço de destino.
- 2 bytes: descrevem o número total de bytes a serem transmitidos.

A soma desses bits faz o controle de colisão nas transmissões, mecanismo que ocorre da seguinte forma:

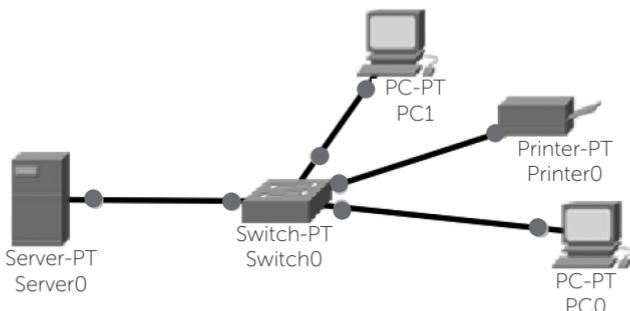
1. Ao ocorrer uma colisão, os dispositivos emissores param de transmitir os 14 bytes.

2. Esse número diferente de 14 bytes é "escutado" pelos nodos.

3. Uma detecção de colisão é informada para os nodos.

O formato do cabeçalho IEEE 802.3 é apresentado na Figura 3.8:

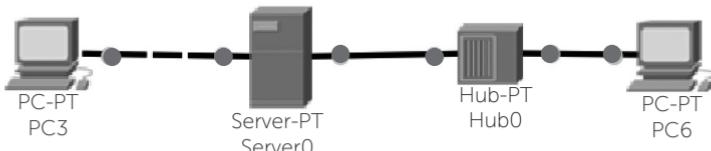
Figura 3.8 | Cabeçalho IEEE 802.3

8 bytes de sincronização			Transmissão 802.3		
Destino	Origem	Total	Dados	PAD	FCS

Fonte: Filippetti (2008, p. 54).

Tais características encontradas no protocolo CSMA/CD fazem com que tenhamos uma Ethernet comutada. Esse tipo de tecnologia é mais recente, o que permitiu uma evolução nas redes do tipo IEEE 802.3.

Ethernet comutada

Segundo Filippetti (2008), essa tecnologia é constituída em cima de uma topologia estrela, estruturada como nodo central um switch (comutador), conforme pode ser observado na Figura 3.9:

Figura 3.9 | Rede estrela com comutador como nodo

Fonte: elaborada pelo autor.

Repare que o "Switch0" é o nodo central que conecta os computadores, o servidor e a impressora. O papel do nodo central de uma rede LAN é ser o comutador dos pacotes que o atravessam. Na comutação, os nodos verificam a porta a que o dispositivo receptor está conectado. Ao descobrir, o comutador pode fazer a transmissão na porta correta, permitindo que as outras portas fiquem livres para efetuar transmissões simultaneamente.

Tais técnicas evitam colisões e permitem velocidades de transmissões do tipo 10/100/100 megabits/s no modo full-duplex. Em

outros tipos de topologia, como em barramento, conforme pode ser observado na Figura 3.10, não se permitem tais velocidades.

Figura 3.10 | Rede em barramento

Fonte: elaborada pelo autor.

Caro aluno, após compreender os conceitos e as características da rede do tipo Ethernet, é possível resgatar o termo "colisão", utilizado em diversas explicações ao longo desta seção.

Tanenbaum (1977) destaca que os dois tipos de ocorrências de colisões nas redes Ethernet são:

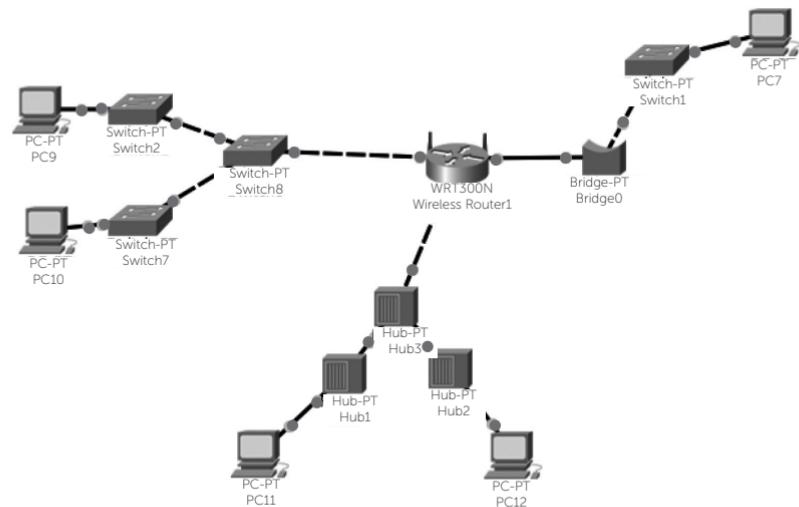
- **Domínio de colisão**

No domínio de colisão, os pacotes têm a possibilidade de efetuar a colisão uns com os outros. Essa ocorrência é um dos fatores principais da degradação dos serviços; se o equipamento que realiza o domínio de colisão for cascateado, a rede pode sofrer maiores consequências.

- **Domínio de broadcast**

No domínio de broadcast, determina-se o limite a que o pacote pode chegar, ou seja, um dispositivo em uma rede local é capaz de efetuar a comunicação com outro sem que seja utilizado um roteador.

Assimile

As mensagens de broadcast são utilizadas pelas operadoras de celular para marketing dos seus serviços oferecidos. Em alguns países são utilizadas para alertas de emergência como enchentes, ameaça de desastres naturais, entre outros.

No entanto, sistemas como Android e IOS podem ser bloqueados para não receber tais mensagens de broadcast.

Após a compreensão dos conceitos relacionados aos domínios de colisão e broadcast, observe o comportamento dos equipamentos nesse contexto:

- HUB: como são equipamentos que repetem as mensagens para todas as portas, formam um único domínio de colisão e broadcast.
- Roteador: são dispositivos concebidos na camada 3 do protocolo TCP/IP – por padrão quebram o domínio de broadcast.
- *Switch*: este equipamento é capaz de formar um domínio de colisão em cada uma de suas portas, em um único domínio de broadcast.
- Bridge: este equipamento pode separar domínios de colisão. Como os switchs, formam um único domínio de broadcast.

Dessa forma, para maior compreensão desse conceito, observe a Figura 3.11:

Figura 3.11 | Topologia com domínio de colisão

Fonte: elaborada pelo autor.

Nela observar que, como o roteador pode separar os domínios de broadcast, na topologia apresentada há três domínios. Já para o domínio de colisão, temos que:

- Abaixo do roteador, a topologia é conectada apenas por *hubs*, formando, assim, um único domínio de colisão e broadcast.

- À esquerda do roteador há dois domínios de colisão, pois os dispositivos estão ligados em um *switch*.
- À direita do roteador há um domínio de colisão ligado no único *switch*; portanto são quatro domínios de colisão.

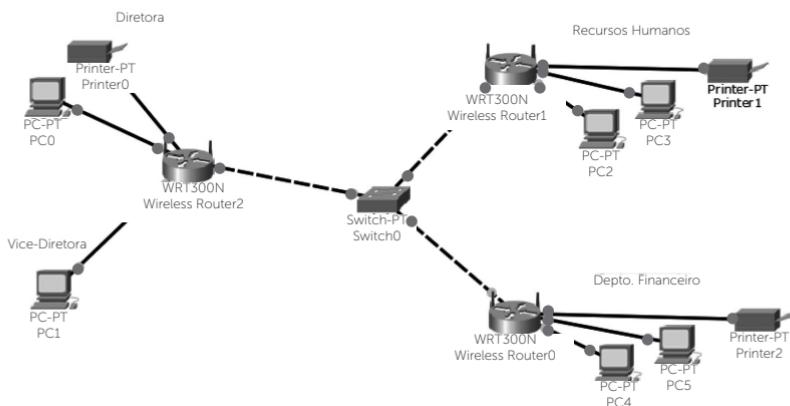
Reflita

Os equipamentos são constituídos em camadas diferentes do protocolo TCP/IP, alguns dos quais formam domínios de colisão e/ou broadcast. A forma como são tratadas as colisões nos diferentes equipamentos pode ser definida segundo a camada em que se atua?

Os estudos e discussões propostos nesta seção permitirão que você possa planejar a estruturação da rede, a fim de ganhar performance para prover os serviços necessários no dia a dia das pessoas e empresas.

Pesquise mais

O artigo de Seixas et al. (2004), intitulado *Implantação de sistema de videoconferência aplicado a ambientes de pesquisa de ensino de enfermagem*, descreve como foi desenvolvido um ambiente multimídia em cima de uma rede Ethernet a fim de prover serviços de videoconferência para prover ensino de enfermagem.

Disponível em: <http://gruposdepesquisa.eerp.usp.br/gepecopen/publicacoes/44614e2c1a6b8f05c538a63a7d099823.pdf>. Acesso em: 10 jun. 2017.

Sem medo de errar

A fim de documentar as experiências nos projetos nas redes de computadores em razão dos quais a equipe resolveu os problemas, o gerente de projetos solicitou que:

- Fossem listados os equipamentos disponíveis em cada um dos setores.
- Fossem calculados os domínios de colisão e broadcast da rede da escola.

Para isso deve ser observada a Figura 3.11, em que:

Figura 3.11 | Topologia da escola Escola 1_A

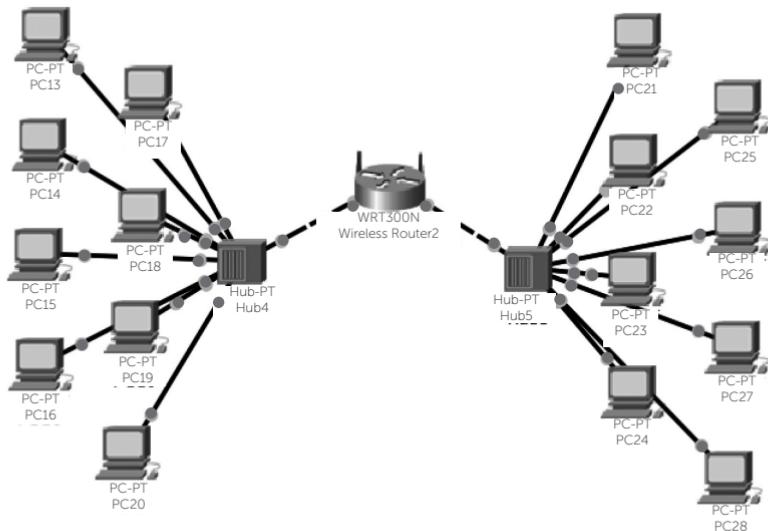
Fonte: elaborada pelo autor.

Para isso:

Lista de equipamentos:

- Direção:
◊ Roteador (wireless Router2).
◊ 2 Desktops (PC0 e PC1).
◊ 1 Impressora (Printer0).
- Recursos Humanos:
◊ Roteador (wireless Router1).
◊ 2 Desktops (PC2 e PC3).
◊ 1 Impressora (Printer1).
- Departamento financeiro:
◊ Roteador (wireless Router0).
◊ 2 Desktops (PC4 e PC5).
◊ 1 Impressora (Printer2).
- Nodo central:
◊ *Switch* (Switch0).

Domínio de broadcast: três domínios, pois cada roteador da topologia forma um domínio de broadcast.

Domínio de colisão: três domínios, pois cada interface de rede do *switch* forma um domínio de colisão. E nessa topologia há os três roteadores (wireless Router0, wireless Router1 e wireless Router2) que se conectam a uma interface de rede do Switch0.

Avançando na prática

Competição de jogo on-line

Descrição da situação-problema

Uma turma de jovens se reuniu para fazer uma competição de jogo on-line. A turma foi dividida em duas equipes, cada uma das quais com oito jogadores. Para isso foi montada a topologia representada a seguir:

Figura 3.12 | Topologia competição de jogo on-line

Fonte: elaborada pelo autor.

Porém, poucos minutos após o início da competição, a rede apresentava lentidão e o servidor ficava indisponível. Para que fosse possível ocorrer a competição, quais equipamentos deveriam ser substituídos? Qual é o motivo de a topologia ter apresentado lentidão e indisponibilidade do servidor?

Resolução da situação-problema

Para que seja possível que a competição aconteça sem que o servidor fique indisponível e sem que ocorra lentidão, caracterizando a degradação do serviço, deve-se substituir os *hubs* de ambos os times (rede do lado direito e esquerdo do Wireless Router2) por um *switch*. Isso ocorre porque os *hubs* são equipamentos que propagam as mensagens para todas as portas, formando, assim, um único domínio de colisão e broadcast, razão pela qual ambos os times estão "inundando" a sua própria rede com mensagens de broadcast "inúteis", ocupando a largura de banda disponível.

Por sua vez, o *switch* pode formar um domínio de colisão em cada uma de suas portas, em um único domínio de broadcast.

Faça valer a pena

1. Na maioria das empresas existem redes de computadores que visam garantir que os recursos sejam compartilhados e diversos serviços sejam providos. Esse tipo de rede pode ser considerado uma rede local (LAN – local area network), caracterizando, assim, uma típica rede Ethernet.
Com base no contexto apresentado anteriormente, observe as afirmativas a seguir:

I. A rede do tipo Ethernet, pode ser definida como Norma 802.8.
II. Na rede Ethernet os dispositivos devem estar conectados em uma mesma linha de comunicação.
III. Os meios de ligação da rede Ethernet devem ser constituídos por cabos cilíndricos.

Assinale a alternativa correta:
a) Somente a afirmativa II é verdadeira.
b) Somente as afirmativas II e III são verdadeiras.
c) Somente as afirmativas I e III são verdadeiras.
d) Somente a afirmativa III é verdadeira.
e) Somente as afirmativas I e II são verdadeiras.

2. O cabeamento estruturado está presente em todas as redes Ethernet, sendo parte muito importante para que os dispositivos possam se comunicar. Tais cabeamentos podem apresentar diferentes características técnicas, que permitem diversas distâncias e velocidades. Essa variedade de cabeamento visa atender às necessidades das empresas.
Observe o texto a seguir:

O tipo de tecnologia aplicada ao cabeamento define as _________________ possíveis nas redes Ethernet, as quais podem ser divididas em ____________ Ethernet, com transmissão de até 100 megabits; Ethernet Gigabit, com transmissão de até 1.000 megabits; e Ethernet 10 Gigabit, com velocidade de 10 ________________.

Assinale a alternativa com a sequência de termos que completa corretamente as lacunas.

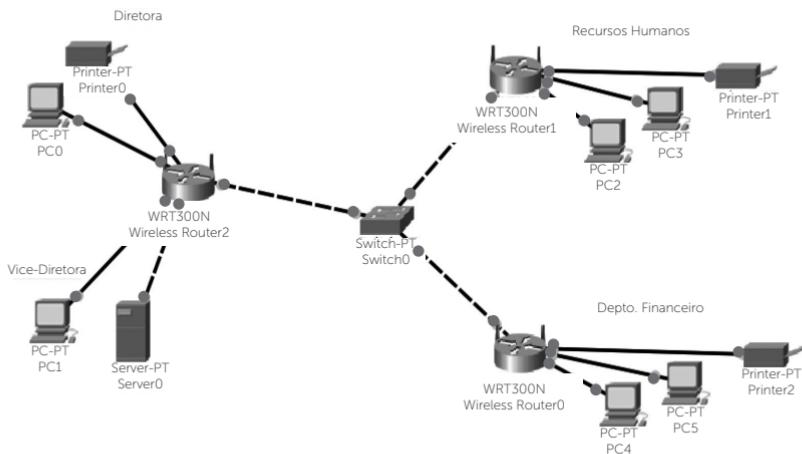
a) velocidades – Big – megabits.
b) distâncias – Fast – bits.
c) velocidades – Fast – gigabits.
d) disponibilidades – Ultra – gigabits.
e) disponibilidades – Big – megabits.

3. As redes locais (LAN) possuem características diferentes das transmissões feitas na WAN (*World Area Network*, rede mundial de computadores). Isso faz com que tenhamos comportamento próprio na comunicação local, protocolo de comunicação projetado para esse fim e tipos de cabeamentos que possibilitam variadas velocidades de transmissão das mensagens de um ponto a outro.

Quanto às características encontradas no protocolo CSMA/CD, indique (V) para as afirmativas verdadeiras ou (F) para as falsas:

( ) No CSMA não persistente, se o meio de transmissão estiver ocupado, a mensagem não é transmitida, sendo descartada.
( ) No CSMA 1 persistente, o dispositivo observa o comportamento da rede até que o meio fique livre e então se inicie a transmissão.
( ) No CSMA p-persistente, o algoritmo calcula a probabilidade de que na transmissão possa ocorrer uma colisão; e, se essa possibilidade for baixa, então ocorre a transmissão.
( ) O mecanismo CD da sigla CSMA/CD faz com que os nodos existentes na rede "escutem" a rede e possam detectar colisões.
( ) O protocolo CMSA/CD não tem a necessidade de hierarquizar a prioridade das transmissões.

Assinale a alternativa com a sequência correta de indicações, de cima para baixo.
a) F – V – V – V – F.
b) F – F – V – V – V.
c) V – F – F – F – V.
d) F – V – F – V – F.
e) V – F – V – F – V.

Seção 3.3

IPv6

Diálogo aberto

A direção da escola Escola 1_A está muito satisfeita com os trabalhos realizados pela sua equipe até o momento. Os gestores, sempre preocupados em manter a qualidade da instituição, solicitaram uma reunião para garantir que a rede da escola tenha boa qualidade para atender às necessidades dos estudantes.

Em razão do grande volume de arquivos gerados pelos departamentos, foi adicionado um servidor na rede, conforme pode ser observado na Figura 3.1:

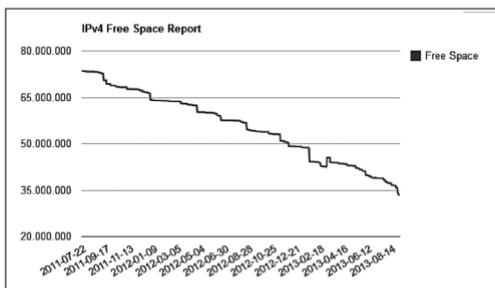
Figura 3.1 | Topologia da escola Escola 1_A

Fonte: elaborada pelo autor.

Porém, como a infraestrutura da escola já contava com as duas versões do protocolo de comunicação IP, configurado nos dispositivos para garantir o acesso aos arquivos, faz-se necessário efetuar a configuração do IPv6 no servidor.

Para isso, você deverá utilizar a técnica de tradução NAT (*Network Address Translation*) no IP destinado ao servidor (172.16.31.55) para que seja posteriormente configurado no dispositivo.

Ao utilizar uma das técnicas que permitem a coexistência e a interoperabilidade entre os protocolos IPv4 e IPv6, você poderá planejar e implementar redes preparadas para atender às necessidades nesse período em que as duas versões do protocolo IP terão que coexistir. Dessa forma, será necessário apresentar os cálculos para conversão de endereço IPv4 para IPv6 no formato de relatório.

O projeto da escola Escola 1_A está chegando ao fim. Você está preparado para enfrentar mais esse desafio?

Não pode faltar

Com o aumento do acesso à internet na maioria dos municípios, os novos serviços multimídia multiplataformas (Smart TV, celular e videogames) e a popularização da internet móvel fizeram que o esgotamento do protocolo IPv4 fosse antecipado, sendo necessário desenvolver uma nova versão do protocolo de comunicação.

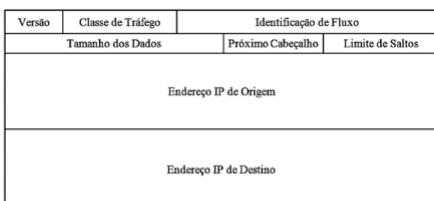
Caro aluno, é dessa necessidade de obter mais endereços que surge o IPv6. O projeto teve início na segunda metade da década de 1990, quando os engenheiros da IETF (*Internet Engineering Task Force* – Força Tarefa de Engenharia de Internet) previam o fim do IPv4.

A LACNIC (*Latin American and Caribbean Internet Addresses Registry*) é um órgão responsável pelos registros de endereços de internet na América e Caribe. Existem outras entidades para o gerenciamento em outros continentes: AfriNIC, ARIN, APNIC e RIPE (Disponível em:<www.lacnic.net>. Acesso em: 20 jun. 2017). A LACNIC foi a responsável por efetuar o monitoramento do esgotamento do IPv4, conforme pode ser observado na Figura 3.16:

Figura 3.16 | Quantidade de IPv4 disponível

Fonte: <www.lacnic.net>. Acesso em: 10 ago. 2017.

Repare que a última data da medição ocorreu em 14/08/2013, quando a LACNIC considerou esgotado o IPv4 (mesmo com um pouco menos de 35.000.000 endereços disponíveis). Por tais motivos e alegações, as empresas como Google, Yahoo e Facebook iniciaram a migração para o protocolo IPv6 em 2010.

Inicialmente o IPv6 surge no cenário de redes de computadores para suprir as necessidades do IPv4. Segundo Tanenbaum (1997), o novo protocolo deve:

1. Resolver a escassez de endereços.
2. Simplificar o cabeçalho, facilitando o processamento dos pacotes e o aumento da velocidade do envio/recebimento.
3. Tornar opcionais os campos obrigatórios do cabeçalho, facilitando, assim, o roteamento dos pacotes.
4. Garantir a segurança das transmissões, tornando o IPsec obrigatório.

Quando os engenheiros se reuniram para o desenvolvimento do novo protocolo, chamado de IPng (*internet protocol next generation* – protocolo de internet da nova geração), as suas características foram definidas por meio das RFCs, disponíveis em: <www.ipv6.br>. Acesso em: 20 jun. 2017. São elas:

- RFC 2460: especificações do IPv6 (12/1998).
- RFC 2461: especificações de descoberta de vizinhos IPv6 (neighbor discovery IPv6).
- RFC 4291: definição da estrutura do IPv6 (01/2006).
- RFC 4443: especificações do ICMPv6 (*internet control message protocol*).

As especificações desenvolvidas pelos engenheiros da IETF para o IPv6 fizeram com que fosse estruturado o cabeçalho demonstrado na Figura 3.17:

Figura 3.17 | Cabeçalho IPv6

Versão	Classe de Tráfego	Identificação de Fluxo	
Tamanho dos Dados		Próximo Cabeçalho	Limite de Saltos
Endereço IP de Origem			
Endereço IP de Destino			

Fonte: <www.ipv6.br>. Acesso em: 20 jun. 2017.

Cada campo tem as seguintes funções:

- **Versão:** indica a versão do protocolo IP utilizada.
- **Classe de tráfego:** indica qual é o nível de prioridade.
- **Identificação de fluxo:** faz o controle de fluxo de informação.
- **Tamanho dos dados:** calcula o tamanho total do datagrama.
- **Próximo cabeçalho:** informa a presença de opções [chama-se de cabeçalhos de extensão].
- **Limite de saltos:** indica número máximo de nós que o pacote pode atravessar.
- **Endereço IP origem:** define o endereço do remetente.
- **Endereço IP destino:** indica o endereço do destinatário.

O endereçamento do protocolo IPv6 possui 128 bits (lembre-se de que o IPv4 possui apenas 32 bits), o que possibilita 2^{128} endereços possíveis, ou ainda 340 undecilhões. O seu formato é dividido em oito grupos com quatro dígitos hexadecimais, conforme pode ser observado: 8000:0000:0010:0000:0123:4567:89AB:CDEF (no IPv4 é dividido em quatro grupos com 8 bits cada, ex.: 192.168.0.100).

Caro aluno, é inevitável neste momento lembrar de que na Seção 3.1 você estudou a versão 4 do protocolo IP, contexto que pode trazer algumas comparações. Segundo Forouzan (2006), os protocolos possuem diferenças entres as duas versões, conforme se observa no Quadro 3.8:

Quadro 3.8 | Adaptado comparativo IPv4 e IPv6

Versão / Itens	IPv4	IPv6
Quantidade de endereços	2^{32}	2^{128}
Quantidade de campos	14	8
MTU mínimo	576 bytes	1.280 bytes
Representação do endereço	4 Grupos com 8 bits	8 Grupos com 16 bits
Tamanho do endereço (bits)	32	128
Roteamento	Tabela de roteamento grande	Efetuado pelo cabeçalho de extensão
Segurança	IPSeg facultativo	IPSeg obrigatório
Qualidade de serviço (QoS)	Sem garantia	Através dos campos, classe de tráfego e identificação de Fluxo
Cabeçalho	Uso do checksum	Mais simplificado

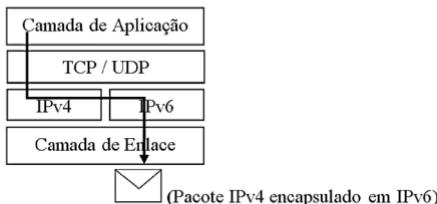
Fonte: Forouzan (2006, p. 255).

O cabeçalho do IPv6 foi simplificado, pois no IPv4 são utilizados 14 campos, enquanto na nova versão do protocolo são utilizados apenas oito deles. Como auxílio visual, repare na Figura 3.17 "Cabeçalho IPv6" e na Figura 3.2 da Seção 3.1, que demonstra o formato do "Cabeçalho IPv4".

Segundo Hagen (2002), IPv6 e IPv4 vão coexistir por muitos anos. E esse novo cenário acabou por gerar um novo problema, pois não é possível "abandonar" o protocolo IPv4 e começar a utilizar somente o protocolo IPv6. Tanenbaum (1997) define que, nesse longo período de transição, os administradores de redes e os provedores de internet preveem que possam ocorrer alguns impactos nas redes, como descrito a seguir:

- **Gerenciamento de falhas**: os administradores devem efetuar um plano de contingência para que as redes continuem operando com o IPv4 e IPv6.
- **Gerenciamento de contabilização**: deve-se recalcular os limites de utilização dos recursos, pois com os dois protocolos em operação o consumo muda em relação as redes somente com IPv4.
- **Gerenciamento de configuração:** para permitir que os dois protocolos possam conviver nas redes, são necessárias diversas configurações.
- **Gerenciamento de desempenho:** com a mudança de cenário (redes com os dois protocolos operando), o desempenho da rede necessita de adaptações para garantia do acordo de nível de serviço (SLA – *service level agreement*).
- **Gerenciamento de segurança:** o administrador deve optar por alguma técnica que garanta a interoperabilidade sem gerar riscos à segurança da rede e/ou de usuários.

Na maioria das redes atualmente é utilizada a primeira versão do protocolo, o IPv4. Apesar da urgência e da escassez da primeira versão, gradualmente os administradores de redes e ISPs (provedores) têm adotado a nova versão do protocolo, o IPv6. No entanto, o que ocorreu com as demais versões do protocolo [IPv1, IPv2, IPv3 e IPv5]?

Caro aluno, em razão da necessidade do período de coexistência entre os dois protocolos, as redes podem apresentar três possíveis cenários: rede IPv4 pura, rede IPv6 pura ou rede com pilha dupla (dual stack). Com isso, a estratégia para migração dos protocolos teve que ser planejada para que o impacto da transição não comprometesse a qualidade dos serviços providos.

Para resolver esse problema, a IETF formou grupo de trabalho denominado IPv6 *Operations* para que fossem desenvolvidas algumas normas e diretrizes para redes IPv4/IPv6. Com isso, o mecanismo de pilha dupla foi normatizado na RFC 1933.

Pilha dupla

Segundo Tanenbaum (1997), os dispositivos que têm a pilha dupla ativada terão dois endereços relacionados à sua interface de rede, um IPv4 e o outro IPv6.

Para que os datagramas possam "atravessar" a pilha dupla, o seguinte mecanismo exposto na Figura 3.18 deve ocorrer:

Figura 3.18 | Mecanismo de pilha dupla

Fonte: elaborada pelo autor.

As mensagens provenientes da camada de aplicação utilizam o encapsulamento na pilha dupla para que sejam enviadas à camada de enlace, que, por sua vez, as conduz à camada física para que, então, sejam enviadas ao meio disponível (cabeado ou sem fio). Nesse sentido, existem duas possibilidades:

1. A mensagem está no formato IPv4 e é encapsulada com IPv6.
2. A mensagem está no formato IPv6 e é encapsulada com IPv4.

Com isso, é necessário que os dispositivos, como computador, servidor, câmera IP, impressoras IP e smartphone estejam com a pilha dupla habilitada.

Exemplificando

A maioria das versões dos sistemas operacionais atualmente (Windows, Linux e MAC) possui suporte a pilha dupla, conforme a Figura 3.19:

Figura 3.19 | Pilha dupla

```
Sufixo DNS específico de conexão. . . . . . :
Endereço IPv6 de link local . . . . . . . . : fe80::2d91:a36e:e649:cff8%11
Endereço IPv4. . . . . . . . . . . . . . . : 192.168.0.103
Máscara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
Gateway Padrão. . . . . . . . . . . . . . . : 192.168.0.1
```

Fonte: elaborada pelo autor.

É possível observar na segunda linha "Endereço IPv6 de link local", o endereço IPv6 atribuído ao dispositivo.

Outra técnica utilizada para permitir a comunicação entre os dispositivos em redes operando com as duas versões do protocolo é empregar o mecanismo de tradução de endereços.

Network Address Translation (NAT)

Definido na RFC 2766, esse mecanismo basicamente é capaz transformar um endereço IPv4 em IPv6 (equivalente). Para isso, devem-se realizar os seguintes passos (considere a conversão do endereço IPv4 192.168.20.112 no exemplo):

1. Converta o endereço IPv4 para binário (a conversão de binário foi definida na Seção 3.2):

11000000 . 10101000 . 00010100 . 01110000

2. Separe os binários em dois grupos de quatro dígitos:

1100 0000 . 1010 1000 . 0001 0100 . 0111 0000

3. Utilize a base "8 – 4 – 2 - 1" para conversão de cada grupo dos binários:

Primeiro grupo:

8	4	2	1		8	4	2	1
1	1	0	0		0	0	0	0

Em que,

1100 = 12

0000 = 0

Segundo grupo:

8	4	2	1		8	4	2	1
1	0	1	0		1	0	0	0

Em que,

1010 = 10

1000 = 8

Terceiro grupo:

8	4	2	1		8	4	2	1
0	0	0	1		0	1	0	0

Em que,

0001 = 1

0100 = 4

Quarto grupo:

8	4	2	1		8	4	2	1
0	1	1	1		0	0	0	0

Em que,

0111 = 7

0000 = 0

4. Converta os números encontrados em cada um dos grupos para hexadecimal:

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

1100 = 12 → C 0000 = 0 → 0, portanto 192 = C0

1010 = 10 → A 1000 = 8 → 8, portanto 168 = A8

0001 = 1 → 1 0100 = 4 → 4, portanto 20 = 14

0111 = 7 → 7 0000 = 0 → 0, portanto 112 = 70

Dessa forma, o endereço 192.168.20.112 é igual a C0A8:1470.

5. Adicione o 0 nos cinco primeiros grupos de 16 bits, seguido de FFFF:

0:0:0:0:0:FFFF:C0A8:1470

Pode-se, ainda em sua forma reduzida, ser representado por ::FFFF:C0A8:1470.

Caro aluno, uma vez configurados os dispositivos nas redes, os nodos devem possuir algum mecanismo que permita a passagem e o roteamento das mensagens, sendo possível ocorrer:

- Nodo IPv4 (IPv4 *only node*): oferece apenas suporte aos dispositivos que aceitem as configurações com o protocolo IPv4.
- Nodo IPv6 (IPv6 *only node*): tem suporte apenas para prover a comunicação IPv6.
- Nodo IPv4/IPv6: possui suporte aos dois protocolos, não necessitando, assim, de nenhuma técnica de transição.

Dessa forma, com exceção do nodo IPv4/IPv6, as demais redes necessitam utilizar alguma técnica para garantir a coexistência e a interoperabilidade entre as duas versões dos protocolos e, consequentemente, o funcionamento correto dos serviços de rede.

6to4

Esta foi a primeira técnica adotada para interoperabilidade entre os protocolos IPv4/IPv6. O mecanismo, definido na RFC 3056, permite que redes IPv6 isoladas consigam se comunicar "roteador a roteador" por túnel automático:

- Roteadores 6to4: devem encaminhar ambos os endereços dos dispositivos clientes.
- Dispositivos clientes: devem estar configurados, pelo menos, com o endereço IPv4.

Tunelamento (*tunneling*)

Determinado pela RFC 2983, fornece orientações técnicas para permitir a utilização de uma infraestrutura IPv4 para encaminhar pacotes IPv6. São estas as possibilidades:

- Roteador a roteador: o pacote IPv6 é encapsulado no início de

sua transmissão, dentro de um pacote IPv4, posteriormente tunelado. Assim, quando atingir o seu destino, efetua o desencapsulamento (a mesma regra vale para tunelamento IPv4 para IPv6).

- Roteador a *host*: um computador IPv4 envia um pacote a um computador IPv6; o pacote, então, atravessa um roteador com suporte à pilha dupla para assim chegar ao seu destino. Para isso, é necessário um túnel entre o roteador e o computador destino.
- *Host a host*: computadores com pilha dupla se comunicam em uma rede IPv4; para isso, o tunelamento ocorre entre os dois computadores.

Túnel *broker*

Este mecanismo foi definido na RFC 3035: o pacote IPv6 é encapsulado dentro do pacote IPv4, permitindo o roteamento através do túnel. Essa técnica normalmente é utilizada em sites IPv4/IPv6 ou em computadores que estejam em uma rede IPv4 e necessitem de interoperabilidade em seus acessos.

ISATAP (*intra-site automatic tunnel addressing protocol*)

Esta técnica foi definida em duas RFCs, sendo elas a 5214 e 4213. Com ela é possível utilizar um endereço atribuído pelo DHCPv4 aos dispositivos, possibilitando que o nodo ISATAP determine a entrada e a saída do túnel IPv6.

Pesquise mais

A Hurricane é uma empresa norte-americana que promove estudos acerca do protocolo IPv6, sendo a única que oferece uma certificação IPv6 (gratuita). Disponível em: <https://ipv6.he.net/certification/>. Acesso em: 22 de jun. 2017.

No Brasil, o IPv6.br mantém cursos, eventos, livros gratuitos para download, vídeos e demais materiais. Disponíveis em: <http://ipv6.br/>. Acesso em: 22 de jun. 2017

Caro aluno, com esses conhecimentos é possível projetar redes que tenham suporte às duas versões do protocolo IP, sendo, por isso, uma infraestrutura preparada para atender às novas tecnologias disponíveis nas redes de computadores.

Sem medo de errar

A escola Escola 1_A, como uma instituição que se preocupa em estar sempre alinhada com o que há de mais atual, já utilizava em sua rede os protocolos IPv4 e IPv6. Porém, para gerenciar e arquivar o grande volume de informações e documentos, foi adicionado um servidor em sua topologia. Para que este possa ser utilizado por todos os dispositivos, é necessário configurar as duas versões do IP (em IPv4 172.16.31.55). Para isso, você deverá utilizar a técnica de tradução (*network address translation*) no IP destinado ao servidor para que seja posteriormente configurado no dispositivo.

Dessa forma, os cálculos utilizados para fazer a conversão do protocolo IPv4 para IPv6 devem ser apresentados em formato de relatório.

a) Conversão do IPv4 para binário.

172 → 10101100

16 → 00010000

31 → 00011111

55 → 00110111

b) Separe os binários em dois grupos.

172 → 1010   1100

16 → 0001   0000

31 → 0001   1111

55 → 0011   0111

c) Passe-os para a base “8 – 4 – 2 - 1” na conversão de cada grupo dos binários:

1010 = 10	1100 = 12
0001 = 1	0000 = 0
0001 = 1	1111 = 15
0011 = 3	0111 = 7

d) Transforme os valores encontrados em hexadecimal.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

172 → AC

16 → 10

31 → 1F

55 → 37

E) Agrupe-os e adicione os complementos "0:0:0:0:0" e ":FFFF".

0:0:0:0:0:FFFF:AC10:1F37

Com a técnica de tradução de endereços, é possível configurar o servidor com as duas versões do protocolo e permitir, assim, a interoperabilidade e a coexistência dos dois protocolos de comunicação. Essas técnicas auxiliarão você a planejar redes que atenda a todas as necessidades de se comunicar nas redes, independentemente da versão utilizada do IP.

Avançando na prática

NET@RTG

Descrição da situação-problema

A NET@RTG é uma empresa especializada em redes de computadores e possui uma grande carteira de clientes. Um dos seus clientes provê jogos on-line, razão pela qual tem a necessidade de ter diversos servidores espalhados pelos países. Na última semana, um dos seus servidores apresentou indisponibilidade: ao abrir um chamado foi indicada a necessidade de um mecanismo de transição em sua topologia.

Uma vez que esse cliente é de sua responsabilidade, o diretor de TI solicitou a você um quadro que descreva os mecanismos de transição disponíveis (com as colunas nome do mecanismo, RFC e característica).

Resolução da situação-problema

Para auxiliar a resolver o problema de falta de mecanismo de transição para a empresa de jogos on-line, o diretor da NET@RTG solicitou que você apresentasse um quadro para que ele pudesse tomar a decisão de qual tecnologia aplicar na topologia.

O resultado foi o seguinte:

Nome do mecanismo	RFC	Característica
Tunelamento (*tunneling*)	2983	Permite a utilização de uma infraestrutura IPv4 para encaminhar pacotes IPv6. São possíveis: Roteador a Roteador, Roteador a *Host, Host a Host*.
Túnel *broker*	3035	O pacote IPv6 é encapsulado dentro do pacote IPv4, o que permite o roteamento através do túnel.
ISATAP (*intra-site automatic tunnel addressing protocol*)	5214 e 4213	O endereço é atribuído pelo DHCPv4 aos dispositivos, o que possibilita que o nodo ISATAP determine a entrada e a saída do túnel IPv6.

Faça valer a pena

1. No final dos anos 1970, quando os engenheiros estavam projetando o IP (*Internet Protocol*), não se previa que haveria diversos serviços disponíveis na rede mundial de computadores. Esses e outros motivos contribuíram significativamente para a escassez de endereços.
Com base nisso, a IETF projetou e desenvolveu um novo protocolo que atendesse às novas demanda das redes, o IPv6.
Inicialmente, a intenção da IETF era suprir a necessidade de endereço, razão pela qual o protocolo IPv6 foi projetado com 128 bits, divididos em oito grupos com quatro dígitos hexadecimal.
Dessa forma, a quantidade possível de endereçamento é de:

a) 2^{128}, ou seja, 34 undecilhões.
b) 2^{32}, ou seja, 40 undecilhões.
c) 2^{128}, ou seja, 340 undecilhões.
d) 128^{2}, ou seja, 3 undecilhões.
e) 2^{12}, ou seja, 30 undecilhões.

2. É muito comum os produtos e serviços passarem por atualizações para corrigir falhas, adicionar ou retirar funcionalidades ou, ainda, sofrer alterações que acabam por mudá-los completamente em relação à sua versão original.

Nas redes de computadores não foi diferente: com a escassez de endereços, depois do IPv4 surge uma nova versão: o IPv6.

Com base no contexto apresentado, observe o quadro a seguir, em que se comparam as duas versões do protocolo IP:

Versão / Itens	IPv4	IPv6
Quantidade de endereços	2^{32}	2^{128}
Quantidade de campos	14	
MTU mínimo	576 bytes	1.280 bytes
Representação do endereço		8 Grupos com 16 bits
Tamanho do endereço (bits)	32	
Roteamento	Tabela de roteamento grande	Efetuado pelo cabeçalho de extensão
Segurança	IPSeg facultativo	
Qualidade de serviço (QoS)	Sem Garantia	Através dos campos Classe de Tráfego e Identificação de Fluxo
Cabeçalho	Uso do Checksum	Mais simplificado

Assinale a alternativa com a sequência que complete corretamente os espaços em branco do quadro (de cima para baixo):

a) 16 – 4 Grupos com 4 bits – 64 – IPSeg obrigatório.
b) 32 – 4 Grupos com 32 bits – 32 – Sem IPSeg.
c) 8 – 8 Grupos com 4 bits – 128 – Sem IPSeg.
d) 8 – 4 Grupos com 8 bits – 128 – IPSeg obrigatório.
e) 32 – 4 Grupos com 16 bits – 32 – IPSeg alternativo.

2. Ao projetar um novo protocolo para atender às necessidades das redes de computadores, acabou-se por gerar um novo problema: as duas versões do protocolo IP terão que coexistir. Isso ocorreu porque não é possível abandonar imediatamente o protocolo IPv4 e todos os dispositivos ficarem aptos a utilizar a nova versão, o IPv6.

Para que o período de coexistência e interoperabilidade possa ser superado,

sem que haja perda da qualidade de serviços, Tanenbaum (1997) define que, no período de transição, os administradores de redes e os provedores de internet devem atentar para:

a) Gerenciamento de mudanças, gerenciamento de gravação, gerenciamento de configuração, gerenciamento de desempenho e gerenciamento de segurança.
b) Gerenciamento de falhas, gerenciamento de contabilização, gerenciamento de manutenção, gerenciamento de alterações e gerenciamento de segurança.
c) Gerenciamento de falhas, gerenciamento de contabilização, gerenciamento de configuração, gerenciamento de desempenho e gerenciamento de coexistência.
d) Gerenciamento de interoperabilidade, gerenciamento de contabilização, gerenciamento de configuração, gerenciamento de desempenho e gerenciamento de coexistência.
e) Gerenciamento de falhas, gerenciamento de contabilização, gerenciamento de configuração, gerenciamento de desempenho e gerenciamento de segurança.

Referências

COMMER, D. E. ***Computer and networks internet with internet applications***. São Paulo: Artmed, 2007.

FILIPPETTI, M. A. **CCNA 4.1:** Guia completo de estudos. Florianópolis: *Visual Books*, 2008. Pág. 54, 57, 147 e 153.

FOROUZAN, A. **Comunicação de dados e redes de computadores.** Porto Alegre: Bookman, 2006.

HAGEN, S. **IPv6 Essentials.** California: O'Reilly Media, 2002.

KUROSE, J. F. **Redes de computadores e a internet:** uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

TANENBAUM, A. S. **Redes de computadores.** 4. ed. Rio de Janeiro: Campus, 1997.

Gerência de redes e padrões

Convite ao estudo

Caro aluno, entramos neste momento na última unidade dos estudos relacionados à rede de computadores. Evoluímos os nossos conhecimentos passando pelos equipamentos utilizados nas infraestruturas, pelo modelo de referência OSI, pelos protocolos de comunicação, entre diversos outros assuntos que proporcionaram uma boa compreensão das características das redes encontradas ao redor do planeta.

Na Seção 4.1, você compreenderá os aspectos técnicos relacionados ao gerenciamento das redes de computadores e a forma como eles se aplicam no dia a dia. Com isso, será possível estudar os padrões de gerência e elementos CMISE/CMIP (*Common Management Information Service/ Commonmanagement Information Protocol*), RMON (*Remote Network Monitoring*), SNMP (*Simple Network Management Protocol*) e TMN (*Telecommunications Management Network*). Por fim, você verá uma discussão sobre algumas técnicas de *sniffing*.

Na Seção 4.2, serão abordados assuntos relacionados a falhas *versus* erros, comumente encontrados nas redes diariamente. Por fim, você compreenderá a importância do monitoramento, da manutenção e da correção nos equipamentos, serviços e usuários, entendendo como os mecanismos de prevenção, como criptografia, auditoria, logs de registros e o controle de acesso podem contribuir para uma rede mais segura.

Na Seção 4.3, serão abordados assuntos relacionados à QoS (*Quality of service* – qualidade de serviços) de redes. Para isso, serão discutidos alguns indicadores, como vazão, nível

de utilização, perfil de tráfego de rede, gargalos, latência e jitter. Isso permitirá a compreensão de como o planejamento correto pode evitar a degradação dos serviços. Por fim, você entenderá a aplicação e a necessidade de efetuar um VLAN Trunk em uma rede.

Chegamos, enfim, ao último nível de conhecimentos relacionados a redes de computadores. Ao promover discussões e estudos acerca de gerenciamento de redes e qualidade de serviços, você estará no caminho para garantir que as redes atendam às necessidades de comunicação das pessoas.

Está pronto para a sua última jornada de estudos a respeito de redes de computadores? Então vamos aos estudos.

Seção 4.1

Teoria da gerência de redes e padrões

Diálogo aberto

Os projetos desenvolvidos pela sua equipe têm refletido em muitas indicações. Os produtos da empresa T2@T Visão, que faz armação para óculos, são comercializados em diversos países europeus. No entanto, a sua rede pode ser considerada uma SOHO (*small office home office* – rede doméstica ou de pequeno escritório).

A rede não possui nenhum sistema de gerenciamento dos dispositivos e serviços utilizados, razão pela qual se geram algumas falhas no monitoramento.

O administrador da rede solicitou uma consultoria para a sua equipe, pois algumas semanas atrás foi determinado que os colaboradores não poderiam mais utilizar *streaming* de vídeo na rede da empresa, uma vez que tais serviços de rede estão consumindo boa parte dos recursos (largura de banda) disponíveis.

Apesar dos comunicados e das reuniões, o administrador de redes não tem certeza se os colaboradores estão ou não conseguindo utilizar tais serviços. Para garantir que os serviços de *streaming* não sejam utilizados dentro da rede, a gerência da T2@T Visão solicitou que a sua equipe apresentasse um relatório que contivesse a indicação de uma ferramenta que pudesse efetuar o monitoramento da rede, de forma a supervisionar os serviços utilizados.

Indicar algumas soluções para os problemas ocorridos nas redes é uma tarefa que requer conhecimento das técnicas adequadas. Você está preparado para resolver mais uma questão relacionada às redes de computadores? Vamos lá.

Não pode faltar

Caro aluno, após estudarmos como as redes são planejadas no nível físico e lógico, é necessário um estudo acerca das técnicas de gerenciamento utilizadas para garantir o funcionamento correto dos serviços. É preciso, ainda, promover uma discussão a respeito dos conceitos e aplicações do *sniffing* nas redes de computadores.

Mas, antes de iniciarmos os conceitos relacionados às técnicas empregadas nas redes de computadores, vamos pensar: Por que gerenciar uma rede de computadores?

Segundo Kurose (2006), o gerenciamento em redes pode ser definido como algumas ações de coordenação dos dispositivos físicos (computadores, servidores, nodos, etc.) e lógicos (protocolos, endereços e serviços), visando garantir a confiabilidade dos seus serviços, um desempenho aceitável e a segurança das informações.

Ainda, segundo Kurose (apud SAYDAM, 1996), as atividades de gerenciamento de redes visam oferecer, integrar e coordenar os elementos de hardware, software e usuários, a fim de monitorar, testar, consultar, configurar, analisar, avaliar e obter o controle dos recursos da rede, para que sejam atendidas as necessidades peculiares de cada rede, com um custo razoável.

A gerência de rede pode ser feita de duas formas básicas:

1. Sistema único de gerência: são um conjunto de ferramentas de monitoramento e/ou controle de dispositivos e/ou serviços, integrados em uma única aplicação.

2. Diversos sistemas de gerência: são ferramentas de monitoramento ou controle de dispositivos ou serviços. Normalmente as ferramentas possuem funções específicas, auxiliando os administradores de redes no monitoramento de diversos serviços. Exemplo: geolocalização de dispositivos da rede (com status ativo ou inativo), monitoramento de tráfego (para efetuar o balanceamento de carga), monitoramento de segurança, entre outros.

Os gerenciadores de rede são ferramentas muito importantes para os administradores de redes. Esses artifícios são os "olhos" dos profissionais de telecomunicações. Os dados dos agentes gerados para os gerentes permitem a tomada de decisão para a garantia da QoS (*quality of service* – qualidade de serviço).

Para que o gerenciamento possa ter elementos para garantir o seu correto funcionamento, Kurose (2006) aponta três princípios:

- Coleta de dados: define-se como a parte do processo responsável por coletar automaticamente dados parametrizados pelo administrador de redes. Nesta seção será vista a técnica definida como *sniffing*.
- Análise e diagnóstico: consiste em organizar os dados coletados a fim de gerar informações que permitam a tomada de decisão. A análise pode ser feita manualmente, ou ainda por softwares de tratamento de dados. A intenção é um diagnóstico correto do problema para que seja feita a correção no menor tempo possível.
- Controle: após o diagnóstico correto do problema, deve-se tomar ações a fim de cessar, mitigar ou minimizar os impactos. E, posteriormente, o administrador de redes deve ter o controle para que o mesmo evento não comprometa a qualidade ou funcionamento da rede e/ou serviços.

Caro aluno, dessa forma nós conseguimos perceber as necessidades de gerenciar as várias competências envolvidas nas redes de computadores. É lógico que, como você deve ter percebido, essa tarefa não é tão simples. Para auxiliar nesse processo, é necessário seguir padrões de qualidade para a garantia de um gerenciamento eficiente.

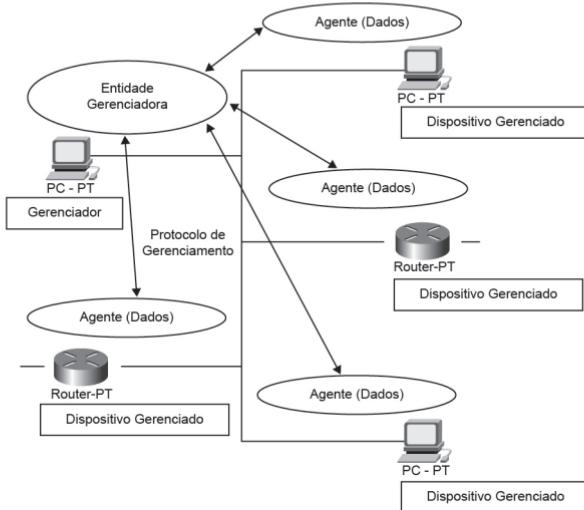
Para isso, segundo Kurose (2006), a ISO (*Internacional Organization for Standardization*) desenvolveu um modelo de gerenciamento de redes, divididos em cinco áreas. São elas:

- Gerenciamento de desempenho: o objetivo é quantificar, medir, informar, analisar e controlar o desempenho de dispositivos, serviços e segurança. Nesse contexto, será visto mais à frente o protocolo SNMP (*Simple Network Management Protocol* – Protocolo Simples de Gerenciamento de Rede).
- Gerenciamento de falhas: visa registrar, detectar e reagir às falhas ocorridas nas redes. O compromisso maior é tratar de imediato as falhas transitórias da rede. Isso ocorre diariamente, quando há interrupções de serviços, hospedagem, falha de hardware e softwares de nodos.
- Gerenciamento de configuração: permite que o administrador saiba quais são os dispositivos utilizados na rede e as suas

respectivas configurações. Nessa área de gerenciamento estão contidos o planejamento dos IPs e as sub-redes.

- Gerenciamento de contabilização: permite a especificação, o registro e controle de acesso (para usuários e dispositivos). Também estão definidas as quotas de utilização (balanceamento de carga conforme prioridade).
- Gerenciamento de segurança: é efetuar o controle de acesso aos recursos via mecanismos de segurança (chaves), métodos de mascaramento de mensagens (criptografia) e políticas de prevenção e segurança.

Reflita

As preocupações referentes à segurança das informações são alvo de diversos debates. Cada vez mais as empresas investem em mecanismos para garantir a privacidade dos seus dados e aplicações.

Um simples pen drive, quando utilizado em um computador localizado em uma empresa, pode comprometer o funcionamento de recursos e serviços?

São diversas as áreas de gerenciamento com as quais o administrador de redes deve se preocupar para garantir a disponibilidade dos recursos da rede e evitar a degradação dos serviços. Caro aluno, é lógico que utilizar softwares de monitoramento nas estações de trabalho pode auxiliar nessa tarefa, pois tais dispositivos podem transmitir em tempo real o status do que está sendo monitorado.

Porém, em redes grandes ou complexas (devido ao número de servidores, serviços, etc.), ter um único gerente para todas as cinco áreas apontadas anteriormente é inadequado, uma vez que diariamente são gerados proporcionalmente grandes volumes de informações pelas necessidades diárias que as redes de computadores apresentam.

Para Kurose (2006), a estrutura do gerenciamento de redes deve possuir os elementos apontados na Figura 4.1.

Figura 4.1 | Principais componentes de uma arquitetura de gerenciamento de redes

Fonte: Kurose (2006, p. 576).

Essa estrutura tem os seguintes componentes:

- Entidade gerenciadora: é o meio pelo qual o administrador de redes interage com a interface de gerenciamento, podendo realizar as atividades de coleta de dados, processamento, análise para posterior tomada de decisão. É tida pelos profissionais de redes como a estação central de gerência de rede.
- Dispositivo gerenciado: é um dispositivo situado em uma rede gerenciada, o qual pode ser monitorado, ex.: servidores, sensores, *switches*, etc. Dentre os objetos gerenciáveis estão os hardwares (placa de rede, por exemplo) e os softwares (aplicações web, por exemplo).
- Protocolo de gerenciamento de rede: é executado entre a entidade gerenciadora e os dispositivos gerenciados, permitindo que os agentes possam informar a entidade gerenciadora sobre a ocorrência de falhas ou violação de algum parâmetro.

Os objetos gerenciados dentro da rede devem fornecer dados para a base de informações encontrada na entidade gerenciadora.

Isso só é possível porque, em cada dispositivo, existe um agente de gerenciamento de rede (software de gerenciamento de rede propriamente dito) que executa testes e envia os resultados para a estação central de gerência de rede.

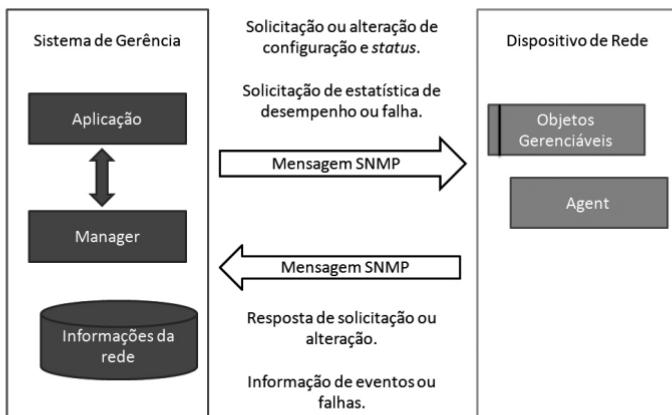
Por sua vez, tais comunicações entre os dispositivos gerenciados e a entidade gerenciadora só ocorre porque o protocolo de gerenciamento de rede permite que aconteçam as investigações, que visam fornecer dados para o administrador de redes garantir o bom funcionamento dos dispositivos e serviços.

Caro estudante, a arquitetura de gerenciamento de redes apresentada anteriormente fornece genericamente parâmetros para obter um gerenciador aplicável na maioria das redes. No entanto, ela ainda não oferece elementos que visam garantir a padronização do gerenciamento das redes de computadores.

Para resolver tais necessidades, no final dos anos 1980, alguns protocolos de gerenciamento começaram a ser oferecidos aos fabricantes. Entre alguns deles, podemos destacar:

SNMP (*Simple Network Information Protocol*)

O protocolo SNMP (*Simple Network Information Protocol* – Protocolo Simples de Gerenciamento de Rede) é definido pela RFC 3410 (disponível em: <https://www.ietf.org/rfc/rfc3410.txt>, acesso em: 7 jul. 2017). A sua primeira versão (SNMPv1) foi lançada em abril de 1999. Hoje é utilizado o protocolo SNMPv3, atualizado em dezembro de 2002.

É, basicamente, um protocolo empregado para efetuar o monitoramento dos dispositivos de redes e os serviços. Por ser popular entre os fabricantes, permite que dispositivos com diversas arquiteturas e sistemas operacionais possam utilizá-lo. Para que ele possa atuar na rede, necessita de quatro componentes básicos:

- Os nodos gerenciados (agentes).
- As estações de gerenciamento (gerente).
- As informações de gerenciamento (MIB*).
- O protocolo de gerenciamento (SNMP).

* MIB (*Management Information Base*) é um banco de dados (lógico) que efetua o armazenamento de informações de

configuração e status, dos dispositivos gerenciáveis. Podem ainda fornecer informações como: nome, atributos e possíveis operações realizáveis.

Para compreender os processos envolvidos no SNMP, observe a Figura 4.2:

Figura 4.2 | Funcionamento do SNMP

Fonte: <https://goo.gl/hGF6Hp>. Acesso em: 7 jul. 2017.

Veja que o SNMP é instalado nos dispositivos gerenciáveis da rede (computador, impressora, câmera IP, etc.), agentes esses que se comunicam diretamente com o MIB e respondem às solicitações efetuadas pelo gerente. Caso ocorra algum evento anômalo, uma notificação (*trap*) é enviada ao gerente.

CMISE *(Commom Management Information Service Element)*

O protocolo CMISE é formado por dois outros protocolos: CMIS e CMIP. Assim, para poder entendê-lo, é necessário conceituar:

- CMIS (*Common Management Information Service*): basicamente define como os serviços serão oferecidos às aplicações de gerenciamento (agente e gerente). Para isso foi definido em três categorias. São elas:

◊ Serviços de associação: utilizados para estabelecer as associações que permitam que ocorram as comunicações entre agente e gerente.

◊ Serviços de notificação: é o mecanismo utilizado para informar os eventos (falhas, por exemplo) ocorridos nos dispositivos gerenciados.

◊ Serviços de operação: permite que o gerente altere as variáveis do MIB, em que é possível utilizar três mecanismos:

  - Escopo: são os parâmetros determinados pelo gerente para que seja determinado o grupo que será alvo do gerenciamento.

  - Filtragem: faz a filtragem no grupo de objetos determinado no escopo.

  - Sincronismo: define quem do grupo estará sobre as regras do gerente, de acordo com o valor definido na mensagem de troca das operações.

- CMIP (*Common Management Information Protocol*): é um protocolo de gerenciamento que segue o modelo de referência OSI. Assim como o SNMP, as trocas das informações seguem a mesma estrutura entre o gerente e o agente nos processos de sistema de gerenciamento. A sua aplicação visa garantir a execução de algumas ações com base na definição de um escopo (filtro) para que os objetos sejam selecionados.

◊ Vantagem: o ponto forte desse protocolo é a segurança.

◊ Desvantagem: utiliza grande parte da capacidade dos sistemas, não sendo possível implementá-lo em todos eles. É de difícil programação, o que o impede muitas vezes de ser utilizado em alguns projetos.

Os tipos de mensagens recebidas/enviadas levam em consideração o CMIS, fornecendo a especificação dos serviços que tanto o sistema gerenciador, quanto os dispositivos gerenciados poderão acessar para que ocorra o gerenciamento.

Pesquise mais

O NIC.br é o núcleo de informação e coordenação brasileiro. O intuito desse grupo é implementar as decisões e os projetos do CGI.br, que

é o Comitê da Internet no Brasil. Entre diversos materiais (apostilas, vídeos e artigos), pode-se destacar o vídeo intitulado *Introdução ao Gerenciamento de Redes*, no qual é demonstrado, de maneira divertida, o funcionamento das ferramentas de gerenciamento.

Disponível em: <https://www.youtube.com/watch?v=TMZVAc8cVnU>. Acesso em: 7 jul. 2017.

TMN (*Telecommunications Management Network*):

Este modelo de gerenciamento está estruturado em três arquiteturas, que podem ser implementadas juntas ou separadas, conforme a necessidade do administrador de rede. São elas:

- Arquitetura informacional: assim como o CMIS, as informações são trocadas entre agente e gerente por meio de um protocolo de gerência de rede. Entretanto, não é utilizado somente um protocolo para prover o gerenciamento, uma vez que cada interface definida na arquitetura física pode utilizar um protocolo adequado à necessidade.
- Arquitetura funcional: esse modelo tem como objetivo definir quais serão as funções e os objetivos na gerência de rede, com os seguintes blocos adicionados: sistema de suporte à operação (OSF); elemento de rede (NEF); estação de trabalho (WSF); adaptador Q (QAF); elemento mediador (MF); e rede de comunicação de dados (DCN).
- Arquitetura física: são definidas as interfaces que garantem a compatibilidade dos dispositivos, as quais são divididas em:

◊ Interface Q: entre os blocos OSF, WSF, QAF, MF e NF.

◊ Interface F: para ligar as estações de trabalho, WSF.

◊ Interface X: entre os blocos OSF, WSF.

◊ Interface G: entre uma QAF e entidade gerenciadas não TMN.

◊ Interface M: entre uma interface QAF e entidades gerenciadas não TMN.

Sniffig:

Segundo o dicionário WordReference, a palavra *sniff* significa farejar. Na prática, é uma ferramenta que efetua a interceptação e o registro dos dados. Em alguns casos é possível decodificar o conteúdo dos pacotes capturados. Esse artifício é utilizado pelos administradores de rede para checar se uma rede está trabalhando dentro dos parâmetros definidos.

Um *sniffer* é um programa instalado em um computador (pode ser considerado um servidor), que visa capturar os fluxos especificados em sua configuração, podendo ser: e-mail, logins, textos, histórico de internet, entre outros. A Figura 4.3 representa um dos *sniffers* mais utilizados pelos administradores de rede.

Figura 4.3 | Logotipo Wireshark

Fonte: <https://goo.gl/uVajiL>. Acesso em: 9 jul. 2017.

Exemplificando

Para efetuar captura dos pacotes e a análise dos dados, existem algumas aplicações gratuitas normalmente utilizadas pelos administradores de redes. Veja exemplos:

- *Wireshark*. Disponível em: <https://www.wireshark.org/download.html>. Acesso em: 9 jul. 2017

- *Capsa*. Disponível em: <http://www.colasoft.com/capsa-free/>. Acesso em: 9 jul. 2017.

- *Microsoft Network Monitor*. Disponível em: <https://www.microsoft.com/en-us/download/details.aspx?id=4865>. Acesso em: 9 jul. 2017.

Caro aluno, compreender as ferramentas de gerenciamento de redes de computadores pode auxiliá-lo a garantir o funcionamento dos dispositivos e serviços disponíveis conforme as necessidades de cada infraestrutura.

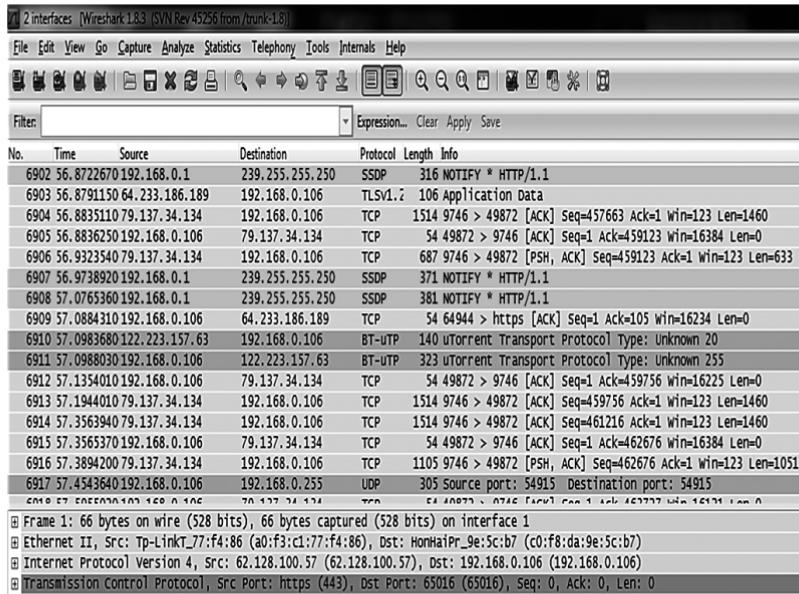
Sem medo de errar

A empresa T2@T Visão faz armação para óculos e possui diversos clientes espalhados por toda a Europa. A sua rede não tem uma topologia tão complexa, razão pela qual também não utiliza protocolos de gerenciamento de rede.

O administrador de redes solicitou uma consultoria, já que foi apresentada uma situação bem comum: a empresa busca mecanismos que proíbam os colaboradores de utilizarem *streaming* de vídeo em sites como: YouTube, Vimeo, Keepvid, etc. O gerente da T2@T Visão fez, então, uma solicitação para que a sua equipe indicasse uma ferramenta que pudesse efetuar o monitoramento da rede para supervisionar os serviços utilizados.

Para tal situação, é preciso que:

Como na rede em questão não é utilizado nenhum protocolo de gerenciamento de rede (sistema de gerenciamento de rede), a indicação para efetuar o monitoramento é o *sniffer*. Essa ferramenta pode permitir ao administrador de redes capturar os pacotes e verificar se algum usuário está utilizando algum serviço não autorizado pela empresa.

Para isso, o mercado possui alguns softwares livres, que auxiliarão na captura dos pacotes, na análise dos dados, ajudando o administrador de redes a monitorar os serviços utilizados pelos colaboradores.

Avançando na prática

Leitura do relatório de *sniffing*

Descrição da situação-problema

Uma rede situada em uma prefeitura possui muitos computadores, localizados em diversas secretarias (educação, segurança, saúde, etc.). Um jovem administrador de redes notou lentidão ao utilizar a internet. Desconfiado de que os colaboradores estariam fazendo downloads na referida rede, ele utilizou um *sniffing* para capturar os pacotes, conforme pode ser observado na Figura 4.4.

Figura 4.4 | Relatório do *sniffing*

2 interfaces [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6902	56.8722670	192.168.0.1	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
6903	56.8791150	64.233.186.189	192.168.0.106	TLSv1.2	106	Application Data
6904	56.8835110	79.137.34.134	192.168.0.106	TCP	1514	9746 > 49872 [ACK] Seq=457663 Ack=1 Win=123 Len=1460
6905	56.8836250	192.168.0.106	79.137.34.134	TCP	54	49872 > 9746 [ACK] Seq=1 Ack=459123 Win=16384 Len=0
6906	56.9323540	79.137.34.134	192.168.0.106	TCP	687	9746 > 49872 [PSH, ACK] Seq=459123 Ack=1 Win=123 Len=633
6907	56.9738920	192.168.0.1	239.255.255.250	SSDP	371	NOTIFY * HTTP/1.1
6908	57.0765360	192.168.0.1	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
6909	57.0884310	192.168.0.106	64.233.186.189	TCP	54	64944 > https [ACK] Seq=1 Ack=105 Win=16234 Len=0
6910	57.0983680	122.223.157.63	192.168.0.106	BT-uTP	140	uTorrent Transport Protocol Type: Unknown 20
6911	57.0988030	192.168.0.106	122.223.157.63	BT-uTP	323	uTorrent Transport Protocol Type: Unknown 255
6912	57.1354010	192.168.0.106	79.137.34.134	TCP	54	49872 > 9746 [ACK] Seq=1 Ack=459756 Win=16225 Len=0
6913	57.1944010	79.137.34.134	192.168.0.106	TCP	1514	9746 > 49872 [ACK] Seq=459756 Ack=1 Win=123 Len=1460
6914	57.3563940	79.137.34.134	192.168.0.106	TCP	1514	9746 > 49872 [ACK] Seq=461216 Ack=1 Win=123 Len=1460
6915	57.3565370	192.168.0.106	79.137.34.134	TCP	54	49872 > 9746 [ACK] Seq=1 Ack=462676 Win=16384 Len=0
6916	57.3894200	79.137.34.134	192.168.0.106	TCP	1105	9746 > 49872 [PSH, ACK] Seq=462676 Ack=1 Win=123 Len=1051
6917	57.4543640	192.168.0.106	192.168.0.255	UDP	305	Source port: 54915 Destination port: 54915

⊞ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 1
⊞ Ethernet II, Src: Tp-LinkT_77:f4:86 (a0:f3:c1:77:f4:86), Dst: HonHaiPr_9e:5c:b7 (c0:f8:da:9e:5c:b7)
⊞ Internet Protocol Version 4, Src: 62.128.100.57 (62.128.100.57), Dst: 192.168.0.106 (192.168.0.106)
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: 65016 (65016), Seq: 0, Ack: 0, Len: 0

Fonte: elaborada pelo autor.

Porém, ao receber o relatório, o administrador não conseguiu definir se estavam sendo utilizados serviços de download nem qual era o IP do dispositivo.

Resolução da situação-problema

O administrador de redes utilizou um software para monitorar os pacotes dos serviços na rede da prefeitura, pois notou lentidão, possivelmente em razão de download feito por algum colaborador. Porém, ao receber o relatório, o administrador não conseguiu determinar qual o serviço de download tinha sido e qual era o IP do dispositivo.

Os pacotes de número 6910 demonstram que o serviço utilizado para download foi o Torrent, ocupando assim a largura da banda pelo dispositivo de IP 192.168.0.106.

Faça valer a pena

1. Em muitos projetos de redes é comum, após a estruturação física da rede e seus respectivos serviços, não ocorrer o gerenciamento. Em diversos casos, os responsáveis enxergam as redes como autogerenciáveis, o que faz com que ocorram falhas e degradação dos serviços.
Quanto às características do gerenciamento em redes de computadores, analise as afirmativas a seguir:
I. Faz o gerenciamento dos dispositivos físicos e lógicos.
II. A monitoração pode garantir a qualidade e disponibilidade dos serviços na rede.
III. Quando eficaz, o gerenciamento monitora apenas o softwares e hardwares utilizados na rede.
Assinale a alternativa correta:

a) Somente a afirmativa II é verdadeira.
b) Somente as afirmativas I e II são verdadeiras.
c) Somente as afirmativas II e III são verdadeiras.
d) Somente as afirmativas I e III são verdadeiras.
e) Somente a afirmativa I é verdadeira.

2. Conforme há o crescimento físico de usuários e serviços, o administrador de redes sente a necessidade de ter ferramentas para auxiliá-lo na tarefa de gerenciamento. Tais artifícios podem tornar erros, falhas e demais ocorrências menos custosos no momento de localizar essas atividades, monitorando-as e resolvendo os problemas no menor tempo o possível.
Observe a frase de Kurose (2006) (apud SAYDAM, 1996):

"As atividades de ______________________ de redes visam oferecer, integrar e coordenar os elementos de hardware, software e ___________________, a fim de se monitorar, testar, consultar, configurar, analisar, avaliar e obter o controle dos recursos da rede, para que sejam atendidas as necessidades peculiares de cada rede, com um _________________ razoável".

Assinale a alternativa que complete as lacunas corretamente:
a) gerenciamento – nodos – tempo.
b) monitoramento – nodos – tempo.
c) gerenciamento – usuários – custo.
d) monitoramento – usuários – custo.
e) acompanhamento – dispositivos – número.

3. O protocolo SNMP é instalado por meio de software em dispositivos gerenciáveis como:

- Computador.
- Impressora.
- *Hub*.
- *Switch*.
- *Bridge*.
- Roteador.

Tais dispositivos são denominados "agentes", que devem se comunicar com o MIB em resposta às solicitações do gerente.

Nem sempre é possível que o administrador esteja presente em todos os setores em que haja algum serviço ou dispositivo, ou ainda estar presente onde se localiza a rede. No entanto, é necessário continuar efetuando o gerenciamento da rede.

Para que o administrador da rede tome ciência das falhas ocorridas, é enviado um "trap" ao gerente, que pode ser definido como:

a) Consulta.
b) Teste.
c) Monitoramento.
d) Gerenciamento.
e) Notificação.

Seção 4.2

Gerência de falhas e segurança

Diálogo aberto

A empresa T2@T Visão é renomada no ramo de armação para óculos graças à qualidade dos seus produtos, diversos dos quais atualmente são comercializados na Europa. A sua rede interna não possui muitos serviços e dispositivos, sendo considerada uma rede pequena.

Para aumentar as vendas, a T2@T Visão faz parceria com algumas empresas de vendas on-line. Para isso, a base de dados do servidor de arquivos da T2@T Visão é compartilhada com essas companhias. Porém, nos últimos cinco dias, os parceiros comerciais informaram ao setor de informática algumas falhas apresentadas:

- Dia 15/05/2017 – 2 falhas, totalizando 60 minutos.
- Dia 16/05/2017 – 1 falha, totalizando 40 minutos.
- Dia 17/05/2017 – 2 falhas, totalizando 80 minutos.
- Dia 18/05/2017 – 1 falha, totalizando 30 minutos.
- Dia 19/05/2017 – 4 falhas, totalizando 90 minutos.

Considerando que um e-commerce deve ficar disponível 24 horas por dia, apresente em forma de relatório ao gerente da T2@T Visão o cálculo de tempo médio entre falhas (MTBF) e tempo médio para reparos (MTTR). Com isso será possível informar para a empresa o tempo total durante o qual o servidor ficou indisponível durante os cinco dias em que foram relatadas as falhas, o que, então, permitirá que seja tomada alguma medida para eliminar ou diminuir a ocorrência de falhas.

Caro aluno, ao efetuar tais cálculos em decorrência das falhas, você poderá efetuar um planejamento de tempo de parada para manutenção, possibilitando mitigar as falhas recorrentes nas redes de computadores.

Pronto para mais esse desafio?

Não pode faltar

Certamente, ao utilizar o serviço de telefonia celular, você já ouviu o eco da sua voz; ou ainda, ao assistir um noticiário pela televisão, percebeu que o áudio e o vídeo perdem o sincronismo entre si. Esses sintomas que causam as degradações dos serviços de comunicação de dados são mais comuns do que pensamos.

Segundo Comer (2007), qualquer sistema de comunicação de dados é suscetível a falhas e erros. Pode ocorrer em dispositivos físicos ou em transmissão. Mesmo quando são feitos exaustivos testes de erros ou de stress de rede, tais ocorrências ainda podem aparecer nas estruturas das redes de computadores. Os erros de transmissão são divididos em três categorias:

- Interferência: são radiações eletromagnéticas que, quando são geradas, podem causar ruído, o que, por sua vez, degrada os sinais de rádio ou os sinais que trafegam pelo meio cabeado.
- Distorção: normalmente os dispositivos físicos de transmissão, como os cabos, fazem a distorção dos sinais. O excesso de distorção de sinais é capaz de causar desde a degradação do serviço até a perda de sinal.
- Atenuação: em meios não guiados, a atenuação se dá quando o sinal necessita atravessar barreiras físicas (parede, vidro, fibra, etc.) e pela distância do receptor da antena. Já no meio guiado, a distância é o fator de degradação dos serviços.

Em redes com uma grande infraestrutura e/ou com diversos serviços disponibilizados aos usuários, é prudente fazer teste de stress, sendo possível determinar:

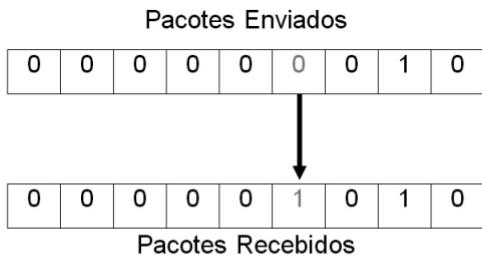
- Quantidade de usuários consecutivos que podem utilizar a rede ou os serviços.
- Capacidade de processamento dos nodos.
- Detecção de colisão.
- Servidores.

Basicamente, são softwares que introduzem uma quantidade de pacotes de tipos e tamanhos diferentes, para que sejam determinados alguns limites e capacidades da rede.

Para a compreensão da taxa de erros encontrados nas redes de computadores, é necessário que conheçamos o Teorema de Shannon. Segundo Carissimi (2009), em 1984 o cientista americano Claude Shannon publicou as bases matemáticas para determinar **a capacidade máxima de transmissão por um canal físico com uma banda passante, em uma determinada relação sinal/ruído**. (Neste momento nos atentaremos apenas para os conceitos, pois os cálculos são tratados nos estudos de telecomunicações.)

Os erros ocorridos na comunicação de dados não podem ser eliminados por completo, porém aqueles relacionados à transmissão podem ser facilmente detectados, permitindo assim que sejam corrigidos automaticamente. Para efetuar o tratamento desses erros existe uma relação de custo-benefício, pois é adicionada uma sobrecarga no processo de transmissão. Os erros de transmissão podem afetar os dados de três formas, conforme demonstrado no Quadro 4.1.

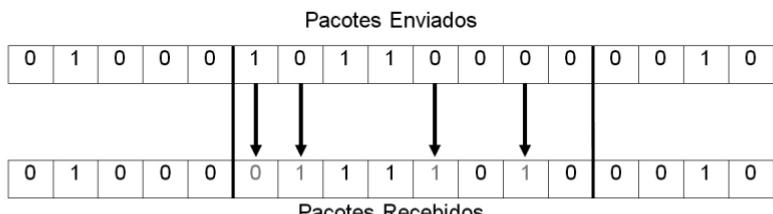
Quadro 4.1 | Erros de dados em sistemas de comunicação

TIPO DE ERRO	DESCRIÇÃO
Erro em um único bit	Apenas um bit sofre uma alteração e os demais permanecem preservados. A degradação do serviço ocorre por um período bem curto.
Erro em rajada	Vários bits sofrem alterações. A degradação do serviço ocorre por um longo período.
Indefinido	A transmissão que chega ao receptor é ambígua (valores fora do escopo). Podem ocorrer diversos períodos de degradação do serviço.

Fonte: Carissimi (2009, p. 120).

Caro aluno, para possibilitar a compreensão do Quadro 4.1, dois termos devem ser mais bem discutidos: "erro em um único bit" e "erro em rajada".

Erro em único bit

Observe na Figura 4.5 a seguir quando o erro ocorre em um único dos bits enviados:

Figura 4.5 | Erro em único bit

Fonte: elaborada pelo autor.

Conforme pode ser verificado, o quinto bit, o mesmo que foi transmitido com o valor “0”, foi recebido pelo valor “1”. O erro de um único bit (single-bit-error) causa uma degradação com menor duração, porém, dependendo do que está sendo transmitido, pode ser mais ou menos degradante, por exemplo: se o erro acontecer quando se está assistindo a um filme por *streaming*, ocorre um travamento momentâneo, ou seja, uma parte da cena é pulada. Por sua vez, se o erro de transmissão ocorre ao tentar acessar um site (transmissão elástico), este apresentará, por exemplo, algum erro de carregamento.

Erros em rajada

Agora observe na seguinte Figura 4.6 a demonstração de quando os erros ocorrem em rajadas:

Figura 4.6 | Erros em rajada

Fonte: elaborada pelo autor.

Não necessariamente os erros em rajada ocorrem em bits consecutivos, conforme pode ser observado na Figura 4.6. Como são transmitidos em rajadas, para contabilizá-los, após a ocorrência de um erro, agrupa-se um bloco de oito bits. Na Figura 4.6 pode-se notar que ocorreram quatro erros.

Os erros em rajada têm um tempo de duração maior em relação ao erro em único bit. Normalmente a degradação do serviço pode ser sensível nas transmissões tanto *streaming*, quanto elástico (acesso a sites, por exemplo).

A comunicação utilizada em jogos on-line é feita em rajada; na ocorrência de erros, em casos mais leves pode apenas apresentar uma paralisação temporária da cena em que o jogo esteja se passando, e, após um tempo retoma-se a partida. Nos casos extremos, quando os erros ocorridos nas transmissões em rajada se repetem continuamente, a conexão pode ser perdida.

As degradações de jogos on-line são muito comuns, pois os erros e as falhas podem ocorrer na transmissão dos dados, no processamento da aplicação no servidor, entre outros casos.

Assim que os erros são detectados, é necessário efetuar a correção deles. No entanto, para que isso ocorra, o número de bits corrompidos deve ser determinado. Nesse caso, são possíveis dois métodos de correção de erros:

- Correção antecipada de erros (FEC – *Forward Error Correction*): são utilizados bits redundantes (por métodos de codificação), possibilitando que o receptor "adivinhe" os bits.
- Correção de erros por retransmissão: quando o receptor encontra um erro, solicita ao emissor para realizar o reenvio da mensagem, processo esse que se repete até que esteja livre de erro.

Caro aluno, certamente todos nós, ao utilizarmos algum serviço, passamos por casos em que o resultado gerado não retornou como o esperado. Tais acontecimentos são chamados de **falhas**. Esse tipo de ocorrência está muito presente na vida das pessoas: quando não se consegue efetuar um saque no caixa eletrônico; quando a

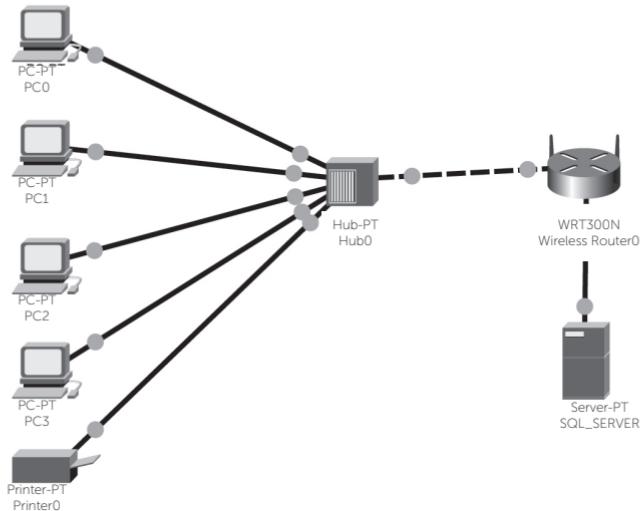
cancela da praça de pedágio não levanta na cobrança automática (Sem Parar, Conect Car, etc.).

Tanenbaum (1997) define que as falhas em sistemas computacionais são respostas incorretas em relação ao que foi projetado como saída, podendo ser definidas por alguns especialistas como defeito. Essas falhas podem ser geradas por fator humano, meios de transmissão, hardware, lógico (software), entre outros.

Para auxiliar os profissionais de tecnologia da informação a prever as falhas de hardware, por meio de análise estatística de dados históricos dos dispositivos de uma rede, são utilizadas as técnicas:

- Tempo Médio Entre Falhas (MTBF – *Mean Time Between Failures*): é uma previsão por modelo estatístico/matemático do tempo médio entre as falhas. É útil para os profissionais de tecnologia da informação, uma vez que prevê as manutenções necessárias. Para realizar o cálculo, utiliza-se:

$$MTBF = \frac{\sum (Final - Início)}{Número\ de\ falhas}$$

- Tempo Médio para Reparos (MTTR – *Mean Time To Repair*): é uma previsão por modelo estatístico/matemático do tempo médio para efetuar reparo após a ocorrência de falha. Para realizar o cálculo, utiliza-se:

$$MTTR = \frac{Tempo\ parado\ por\ falha}{Número\ de\ falhas}$$

Para auxiliar a compreensão, vejamos um exemplo:

1. O servidor disponível na topologia apresentada na Figura 4.7 disponibiliza acesso às informações do sistema da empresa (SQL_SERVER). O horário de trabalho é das 08h às 17h (9 horas), período durante o qual o servidor ficou indisponível quatro vezes, somando o total de uma hora de parada.

Qual é o tempo encontrado entre as falhas? Qual é o tempo necessário para efetuar os reparos?

Figura 4.7 | Topologia de rede em uma empresa

Fonte: elaborada pelo autor.

Para o cálculo do tempo médio entre as falhas, temos que:

$$MTBF = \frac{(9-1)}{4} \rightarrow MTBF = 2\ horas$$

Com isso, é possível determinar o tempo de manutenção de cada uma das paradas:

$$MTTR = \frac{60}{4} \rightarrow MTTR = 15\,\text{min}$$

Ou seja, dessa forma é possível prever, por meio dos cálculos efetuados com os dados históricos/estatísticos, que a cada duas horas o servidor apresentará uma falha e que serão necessários quinze minutos para efetuar a sua manutenção. Dessa forma, o “SQL_SERVER” ficará indisponível por duas horas, durante o turno de trabalho de nove horas.

Reflita

Embora as observações históricas e os tratamentos estatísticos do MTBF e MTTR possam prever os tempos decorrentes de falhas, o tempo de reparo e manutenção, por que, ainda assim, os serviços de internet, bancários, entre outros utilizados no dia a dia, apresentam falhas?

Durante os primeiros anos, a utilização das redes era destinada apenas para pesquisas, trocas de mensagens e compartilhamento de alguns recursos, como as impressoras. Nessas condições, a segurança nunca foi uma preocupação. Com o advento de maior oferta de internet pelas operadoras e consequentemente um maior número de dispositivos, tais implicações passaram a ser uma ameaça para as pessoas e empresas.

Segurança de redes é um assunto muito abrangente, razão pela qual, nesta seção, vamos nos concentrar em criptografia, logs e controle de acesso.

Criptografia

Segundo Tanenbaum (1997), quatro grupos contribuíram para o surgimento e o aprimoramento dos métodos de criptografia: os militares, os diplomatas, as pessoas "comuns" que gostam de guardar memórias e os amantes. O maior volume de contribuição adveio dos militares, uma vez que eles tinham interesses como estratégia de comunicação em período de guerra.

Basicamente, o processo consiste em transformar uma mensagem de texto com uma chave parametrizada, cuja saída é um texto cifrado, com o uso de um algoritmo criptográfico. Se a mensagem for capturada e o interceptor não possuir a chave, este não conseguirá fazer o processo inverso, que possibilite ler o conteúdo da mensagem. Neste momento vale a pena conceituar três termos:

- Criptoanálise: arte de solucionar ("desvendar") as mensagens cifradas.
- Criptografia: arte de criar mensagens cifradas.
- Criptologia: estudos acerca de criptoanálise e os métodos de criptografia.

Tanenbaum (1997) sugere um modelo matemático para representar o processo de criptografia, em que:

$C = E_k(P)$ onde:

P $\rightarrow$ denota o texto simples.

k $\rightarrow$ chave para criptografia.

C $\rightarrow$ texto cifrado.

Para o processo inverso (descriptografia), temos que:

$$P = D_k(C)$$

Essas notações sugerem que as letras "E" e "D" são funções matemáticas. Dessa forma, tanto na função de criptografia, quanto na de descriptografia há uma chave aplicada a uma função matemática.

Pesquise mais

Outra forma de proteger uma mensagem é utilizar a técnica de esteganografia, que pode ser definida como a arte de esconder dentro de outro arquivo aparentemente inofensivo alguma mensagem; se esta for interceptada, não será possível detectá-la.

Para conhecer mais sobre a técnica, leia o artigo de Nunes et al. intitulado *Esteganografia*. Disponível em: <http://www.pgsskroton.com.br/seer/index.php/rcext/article/view/3401/3032>. Acesso em: 15 jul. 2017.

Caro aluno, como as funções matemáticas podem assumir infinitos valores e variáveis, vamos nos concentrar nesse momento nos conceitos relacionados à "chave".

Chave

Segundo Tanenbaum (1997), para a compreensão do conceito de chave no tocante de criptografia é necessário o entendimento do princípio de Kerckhoff. Esse nome é em homenagem ao militar Auguste Kerckhoff que em 1883, publicou que: "Todos os algoritmos devem ser públicos; apenas as chaves são secretas." (KERCKHOFF, 1883 apud TANENBAUM, 1997, p. 546).

Dessa forma, podemos compreender que o algoritmo não necessita ser secreto ou sigiloso. Os fatores relacionados à segurança

devem estar nas chaves, para isso é sugerido que possuam os tamanhos e aplicações conforme demonstrado no Quadro 4.2:

Quadro 4.2 | Tamanho das chaves versus aplicação

Tamanho da Chave	Aplicação
64 bits	Correio eletrônico, mensagens de chat, entre outros meios de comunicação instantânea que não exijam nível específico de segurança.
128 bits	Uso comercial, empresas, universidades, etc.
256 bits	Comunicação de interesse governamental.

Fonte: adaptado de Tanenbaum (1997, p. 547).

Caro aluno, os tamanhos das chaves mudam a cada ano, conforme as quebras se tornam possíveis com o aumento do poder computacional. Em todos os tamanhos das chaves, espera-se que a garantia do sigilo das informações em sistemas computacionais se dê na presença de um algoritmo forte, porém público, e uma chave de longo comprimento.

Logs

Segundo Tanenbaum (1997), são ferramentas importantes para os administradores de redes, pois são recursos de fácil implementação que podem fornecer um histórico para análise. Os geradores de *logs* devem obedecer a uma regra simples: manter os dispositivos sincronizados ao servidor NTP. Tais registros de logs devem ser armazenados em servidores local ou remoto e as suas informações podem ser acessadas on-line e/ou off-line.

Caro aluno, de nada basta gerar e armazenar os *logs* se algumas práticas de monitoramento não forem seguidas:

- A inspeção dos *logs* deve ser uma rotina de trabalho.
- Devem-se investigar as causas dos *logs* (os nocivos à segurança e ao funcionamento da rede).
- Devem-se estabelecer padrões de funcionamento para facilitar a análise dos *logs*.

Controle de acesso

Segundo Tanenbaum (1997), também conhecida como NAC (*Network Access Control*), é um recurso muito importante para

auxiliar no gerenciamento das questões relacionadas à segurança. Tais ferramentas auxiliam o administrador de redes nas seguintes tarefas:

- Controle de acesso à rede, de pessoas e/ou equipamentos não autorizados.
- Evitar intrusões fraudulentas, cujo intuito é o roubo de informações sigilosas.
- Detectar dispositivos vulneráveis ou infectados que possam colocar a rede em risco de alguma forma.

Tais técnicas permitem que os dispositivos e usuários que necessitem conectar-se à rede sejam identificados e, se possuírem credenciais, sejam autorizados a fazê-lo, sendo, portanto, possível verificar o status e a atualização de antivírus, as aplicações, os softwares, etc.

Caro estudante, conhecer todos os conceitos e todas as aplicações abordados nesta seção de ensino garantirá que a rede atenda aos padrões de qualidade desejados, possibilitando o cálculo de tempo de manutenção, a utilização dos métodos de criptografia adequados para cada caso, mostrando, para isso, a importância de se manter o controle de acesso para a garantia da segurança da rede e dos usuários.

Sem medo de errar

A empresa T2@T Visão, que produz armações para óculos, resolveu inovar e fez parceria com algumas empresas de vendas on-line. Para isso, a base de dados do servidor (SQL_SERVER) é compartilhada com essas empresas. No entanto, um problema nesse servidor fez com que os parceiros comerciais relatassem as seguintes falhas:

- Dia 15/05/2017 – 2 falhas, totalizando 60 minutos.
- Dia 16/05/2017 – 1 falha, totalizando 40 minutos.
- Dia 17/05/2017 – 2 falhas, totalizando 80 minutos.
- Dia 18/05/2017 – 1 falha, totalizando 30 minutos.
- Dia 19/05/2017 – 4 falhas, totalizando 90 minutos.

Considerando que um e-commerce deve ficar disponível por 24 horas por dia, o gerente da T2@T Visão solicitou um relatório com o cálculo de tempo médio entre falhas (MTBF) e de tempo médio

para reparos (MTTR). A empresa deseja saber o tempo durante o qual o SQL_SERVER ficou indisponível nos cinco dias em que foram relatadas as falhas.

Temos que, para o cálculo de tempo de operação, devemos fazer 5 (dias) x 24 (horas) = 120 horas.

Somatória do tempo de falhas → 60 + 40 + 80 + 30 + 90 = 300 minutos, ou 5 horas.

Número de falhas → 2 + 1 + 2 + 1 + 4 = 10 falhas.

Para o cálculo do tempo médio entre as falhas, temos que:

$$MTBF = \frac{(120-5)}{10} \rightarrow MTBF = 11,5$$

Ou seja, as falhas ocorrem a cada 11h30.

Com isso, é possível determinar o tempo de manutenção de cada uma das paradas:

$$MTTR = \frac{300}{10} \rightarrow MTBF = 30$$

Ou seja, o tempo utilizado para cada manutenção é de 30 minutos.

Dessa forma, pode-se concluir que a cada 11h30 o servidor fica indisponível por meia hora, ou, ainda, que o SQL_SERVER instalado na topologia da T2@T Visão fica indisponível para os parceiros comerciais uma hora por dia.

Avançando na prática

Escritório de advocacia

Descrição da situação-problema

Um grupo de advogados possui profissionais nas especialidades do Direito para atender as mais diferentes necessidades de seus clientes. No escritório há uma recepção e quatro cômodos, um para cada advogado. O ambiente possui wi-fi para comodidade dos clientes e uma recepção com uma atendente.

A fim facilitar o momento de anunciar a chegada de um cliente para o advogado, o escritório contratou um desenvolvedor para

fazer um chat de comunicação. No entanto, o desenvolvedor não possui experiência em criptografar mensagens em rede, tendo lhe enviado o seguinte e-mail:

> "Em razão de sua experiência em redes de computadores, estou fazendo contato com você para que me indique o tamanho adequado que devo utilizar para desenvolver um chat de uso interno em um escritório de advocacia. Aguardo retorno de sua assessoria em redes."

Resolução da situação-problema

Para auxiliar o desenvolvedor de software na construção do chat de uso interno em um escritório de advocacia, o e-mail foi respondido da seguinte forma:

> "Sr. Desenvolvedor,
>
> Para o desenvolvimento do *chat* de forma que não prejudique o desenvolvimento, você pode utilizar chave de 64 bits, pois, como não são muitos dispositivos conectados na rede, acredito que esse comprimento deva atender às suas necessidades.
>
> Porém, como a sua rede wi-fi é aberta ao público, os dispositivos que se conectam a ela podem causar vulnerabilidade. Dessa forma, se a rede continuar aberta ao público, sugiro que você utilize em sua programação do *chat* chave com o comprimento de 128 bits.
>
> At.te"

Faça valer a pena

1. Falhas e erros são eventos que podem estar presentes em diversos sistemas de comunicação que utilizamos em nosso dia a dia, ao acessar um aplicativo pelo celular, para efetuar um saque no caixa eletrônico, ou ainda ao passar pela cobrança automática no pedágio. Algumas dessas falhas, apesar de provocarem a degradação do serviço, não causam prejuízos maiores, porém outros tipos de falhas podem trazer milhões de prejuízos para uma empresa.

Em redes de computadores existem parâmetros que podem ser determinantes para o aumento/diminuição da taxa de erros. Em 1884 um

cientista americano propôs o teorema de Shannon, por meio de suas bases matemáticas.
Assinale a alternativa que descreva corretamente o teorema de Shannon.

a) O teorema de Shannon descreve que a capacidade mínima de transmissão não guiada com uma banda passante é determinada pela relação de perda de sinal.
b) O teorema de Shannon descreve que a capacidade da banda passante independente do meio de transmissão sofre interferência mínima devido ao aumento do sinal/ruído.
c) O teorema de Shannon descreve que a capacidade máxima do sinal em uma transmissão por um canal físico é determinada pela intensidade do ruído.
d) O teorema de Shannon descreve que a capacidade máxima de transmissão por um canal físico com uma banda passante é determinada pela relação sinal/ruído.
e) O teorema de Shannon descreve que a capacidade máxima do ruído em uma transmissão por meio não guiado é determinada pela intensidade do sinal.

2. Em diversos lugares que frequentamos diariamente existe uma forma de garantir que apenas pessoas autorizadas acessem determinado local. Dentre eles, podemos destacar:
• Porta giratória de banco.
• Catraca de faculdade.
• Portaria de condomínio residencial.
• Catraca de estádio.
O intuito de fazer uma verificação de entrada e saída é o importante controle de segurança. O gerenciamento do controle de acesso de pessoas, veículos, etc. pode ser feito de forma manual ou por sistemas computacionais.
Segundo Tanenbaum (1997), a também conhecida como NAC (*Network Access Control*) é um recurso de controle de acesso utilizado em redes de computadores. Com base nesse contexto, observe as afirmativas a seguir:
I. O controle de acesso pode ser feito no nível de hardware, por exemplo, no bloqueio das portas USB dos computadores.
II. O controle de acesso pode evitar intrusões na rede.
III. O controle de acesso pode evitar que dispositivos infectados se conectem na rede.

Assinale a alternativa correta:
a) Somente as afirmativas I e II são verdadeiras.
b) Somente as afirmativas I e III são verdadeiras.
c) Somente as afirmativas II e III são verdadeiras.
d) Somente a afirmativas III é verdadeira.
e) As afirmativas I, II e III são verdadeiras.

3. Certas profissões exigem, ao profissional que assumir as funções de sua responsabilidade, que seja lido o relatório com as atividades que ocorreram antes do seu turno. Entre algumas profissões, poderíamos destacar:
• Atividades policiais.
• Atividades relacionadas à saúde (enfermagem, resgate, etc.).
• Sistemas de produção.
Nesses relatórios podem ser registrados incidentes, falhas, erros, boas práticas, entre outras informações úteis, para que as atividades possam ser efetuadas com segurança e qualidade.

Nesse contexto, observe o texto a seguir:

O *log* nas redes de computadores é uma importante ferramenta para que seja ________________ um histórico das atividades ocorridas nas infraestruturas. Para a garantia da veracidade dos registros, os geradores de log devem estar sincronizados com um servidor _______________. Essas informações podem ser alocadas em _________________ remotos ou local.

Assinale a alternativa que complete as lacunas corretamente:

a) excluído – NTP – históricos.
b) registrado – NTP – servidores.
c) excluído – HTTP – servidores.
d) registrado – HTTP – históricos.
e) alterado – HTTP – servidores.

Seção 4.3

Gerência de desempenho, configuração e contabilização

Diálogo aberto

A empresa T2@T Visão, especializada em armação para óculos, tem como característica fabricar produtos de qualidade internacional. Atualmente, grande parte da sua produção é comercializada na Europa. Para ampliar as suas vendas, a companhia compartilha a sua base de dados com alguns parceiros comerciais, que fazem a revenda dos seus produtos.

Recentemente a gerência solicitou o cálculo de tempo médio entre as falhas (MTBF – *Mean Time Between Failures*) e o tempo médio para reparos (MTTR – *Mean Time To Repair*), chegando à conclusão de que o serviço fica indisponível uma hora por dia. O tempo anual que a base de dados deve ficar disponível é de 8000 horas (MTTF - *Mean Time to Failure*).

O gerente **solicitou um relatório com o demonstrativo do cálculo de disponibilidade** da base de dados, pois o contrato prevê que ela precisa ser maior que 90%, caso contrário a T2@T Visão deve pagar multa aos parceiros comerciais.

Caro aluno, efetuar os cálculos de disponibilidade de serviços e/ou dispositivos de uma rede de computadores possibilita o planejamento preventivo a fim de garantir o funcionamento sem que haja interrupção.

Vamos ajudar o gerente da T2@T Visão efetuando os cálculos de disponibilidade?

Não pode faltar

Caro aluno, todos nós já utilizamos algum meio de comunicação ou um serviço de rede, que não conseguiu atender com a qualidade esperada. Para que possamos parametrizar alguns serviços, é necessário conhecermos quais são os indicadores utilizados nas redes de computadores a fim de garantir a qualidade e a disponibilidade.

Nível de utilização

Talvez uma das maiores dificuldades encontradas é ajustar os parâmetros de desempenho da rede para que possam suprir as necessidades. Segundo Tanenbaum (1997), em diversas situações os engenheiros de redes necessitam avaliar desde a estrutura da rede até os dispositivos individualmente, para então realizar testes probatórios de qualidade.

Normalmente os testes de desempenho são feitos por meio da injeção de um determinado tráfego na rede, permitindo assim que o administrador de rede analise as saídas. Vários aspectos podem ser observados, tais como, entre outros:

- Taxa máxima suportada.
- Tempo de deslocamento de um pacote.
- Tempo de recuperação a falhas.

Um software muito utilizado por administradores de redes para analisar vazão, latência, *jitter* e perda de pacotes é o Iperf (Jperf em Linux). Esse programa faz a análise de rede e do seu desempenho, por meio das ferramentas disponíveis e configuradas, para enviar pacotes de tamanhos variáveis conforme o experimento a ser realizado.

Disponível em: <https://iperf.fr/iperf-download.php>. Acesso em: 24 jul. 2017.

Ao utilizar esses tipos de ferramentas, é possível compreender quais dados são mais/menos utilizados, qual é o horário de maior consumo dos recursos, entre outras coisas. Isso possibilita a compreensão do perfil dos usuários e adequação da rede a fim de atender aos serviços prioritários para determinada rede.

Perfil de tráfego

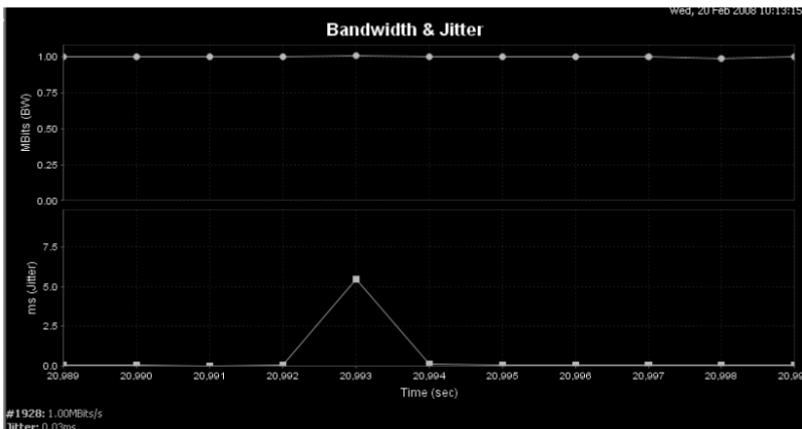
Caro aluno, quando pensamos no quesito "desempenho da rede", não importa muito o tipo de serviço que se esteja utilizando. Porém, nas seções anteriores, quando estudamos os protocolos de

redes, principalmente o TCP/IP e UDP, vimos que todos eles têm funcionamento, tamanho e, consequentemente, ocupam mais/menos recursos da rede.

Tenambaum (1997) define que as redes devem ser reconfiguráveis graças ao fato de os perfis de tráfego mudarem com muita frequência. Para a garantia da continuidade dos serviços da rede e a manutenção da qualidade, os administradores de redes devem permitir:

- Novos serviços.
- Crescimento do tráfego.
- Novas tecnologias.
- Padronização e interoperabilidade entre os protocolos e equipamentos.

Dessa forma, ao conhecer o perfil do tráfego da rede, é possível adequar os recursos às necessidades, ou ainda manter o equilíbrio necessário para ter um nível de qualidade adequado.

Vazão *(Throughput)*

Segundo Forouzan (2006), a vazão em redes de computadores pode ser definida como a quantidade de dados transferidos entre dispositivos (da mesma rede, ou de redes diferentes), ou mesmo a quantidade de dados processados em determinado tempo. Normalmente é expressa em bits por segundo (bps). "Ou seja, se considerarmos o ponto como sendo um plano que secciona o meio, o *throughput* é o número de bits que atravessa esse plano". (FOROUZAN, 2006, p. 90)

Os fatores que interferem na vazão são:

- Topologia de rede.
- Número de usuários.
- Taxa das interfaces de rede.

Observe a Figura 4.8, em que a vazão é medida por meio do software Iperf.

Figura 4.8 | Resultados experimentais de *throughput*

Wed, 20 Feb 2008 10:13:15

Bandwidth & Jitter

MBits (BW)

1.00
0.75
0.50
0.25
0.00

ms (Jitter)

7.5
5.0
2.5
0.0

20,989 20,990 20,991 20,992 20,993 20,994 20,995 20,996 20,997 20,998 20,99

Time (sec)

#1928: 1.00MBits/s
Jitter: 0.03ms

Fonte: elaborada pelo autor.

Na parte superior da Figura 4.8, pode-se observar que a rede está permitindo a utilização de 100% da capacidade de sua vazão.

Dessa forma, podemos concluir que a vazão poderia ser descrita como a velocidade em que os dados realmente trafegam pela rede. Essa taxa de transferência pode ser menor do que a largura de banda, devido a perdas e atrasos.

Perda de pacotes

Segundo Tanenbaum (1997), em razão de os roteadores não terem a capacidade de armazenamento de pacotes infinita, após o esgotamento, os pacotes são descartados. À medida que a rede cresce ou a exigência de processamento aumenta devido às aplicações, o nodo passa a ter mais solicitações e, consequentemente, pode ocorrer perda de pacotes.

Caro aluno, para melhor compreensão de que forma a perda de pacotes pode degradar os serviços, na Figura 4.9 é demonstrado um teste com base no qual é possível observar as perdas de pacotes ocorridas em uma rede.

Figura 4.9 | Resultados experimentais de perda de pacotes 1

```
C:\Users\Prof. Serginho Nunes>ping 192.168.0.1

Disparando 192.168.0.1 com 32 bytes de dados:
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Resposta de 192.168.0.1: bytes=32 tempo=160ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=1948ms TTL=64

Estatísticas do Ping para 192.168.0.1:
    Pacotes: Enviados = 4, Recebidos = 2, Perdidos = 2 (50% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 160ms, Máximo = 1948ms, Média = 1054ms
```

Fonte: elaborada pelo autor.

Propositalmente, utilizando uma conexão sem fio a dez metros do roteador (com o sinal atravessando quatro paredes), houve dois pacotes perdidos. Em outras palavras, 50% do serviço ficou indisponível para os usuários.

Agora observe a Figura 4.10 em que o teste foi feito a dois metros do roteador.

Figura 4.10 |Resultados experimentais de perda de pacotes 2

```
C:\Users\Prof. Serginho Nunes>ping 192.168.0.1

Disparando 192.168.0.1 com 32 bytes de dados:
Resposta de 192.168.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=6ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=4ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=5ms TTL=64

Estatísticas do Ping para 192.168.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1ms, Máximo = 6ms, Média = 4ms
```

Fonte: elaborada pelo autor.

Nesse segundo cenário pode-se observar que 100% dos pacotes foram recebidos.

Latência (atraso)

Segundo Carissimi (2009), em redes de computadores, latência é o intervalo de tempo entre o momento que o emissor enviou o pacote e o recebimento da confirmação do pacote por parte do receptor. O tempo que o receptor gasta no processamento do pacote não deve ser utilizado no cálculo da latência.

A latência pode ser considerada:

Latência = *Tempo de transmissão + Tempo de propagação*

Em que:

• Tempo de transmissão = D*imensão do pacote (bits) / Velocidade da Transmissão (bps).*

• Tempo de propagação = *Dimensão do Canal (Km) / Velocidade de Propagação (Km/s).*

Segundo Kurose (2006), há dois outros tipos de atrasos que podem provocar latência: o tempo de processamento e o tempo de enfileiramento (gargalos). No entanto, esses dois tempos só podem ser aferidos em uma rede com utilização de tráfego significativamente elevado.

Caro aluno, no experimento utilizado para demonstrar a perda de pacotes (observe nas Figuras 4.9 e 4.10), temos um parâmetro de saída do teste com valores para "mínimo", "máximo" e "média", organizados conforme o Quadro 4.3.

Quadro 4.3 | Resultados experimentais de latência (ms)

Valores	Experimento 1	Experimento 2
Mínimo	160 ms	1 ms
Máximo	1948 ms	6 ms
Média	1054 ms	4 ms

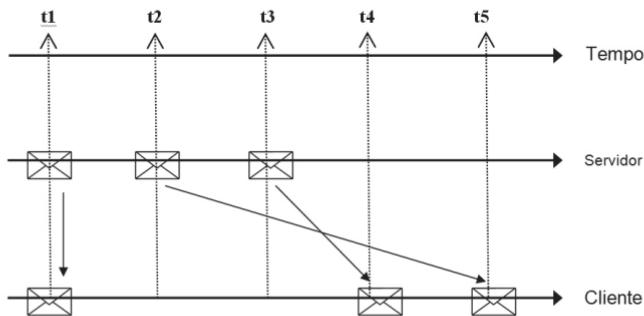
Fonte: elaborado pelo autor.

Foi possível compreender numericamente os experimentos ao observarmos os tempos de propagação dos pacotes.

O aumento da latência (atraso) e a perda de pacotes nas transmissões sofrem interferências devido, entre outros fatores, à:

• Distância entre os nodos.

• Distância da antena (em transmissão sem fio).

• Qualidade dos links (cabeado ou sem fio).

É fato que esses tipos de ocorrências podem se mostrar como um dos maiores degradadores dos serviços encontrados nas redes de computadores.

Jitter

Segundo Comer (2007, p. 43), "o *jitter* pode ser definido como a variação no tempo e na sequência de entrega dos pacotes (*Packet-Delay Variation*) devido à variação da latência (atrasos) na rede". A influência do *jitter* é mais sensível para a qualidade de serviço quando se tem a necessidade da garantia na entrega dos pacotes em períodos definidos.

O *jitter* é analisado na periodicidade na transmissão dos pacotes, como também na variação da entrega dos pacotes, conforme pode ser observado na Figura 4.11:

Figura 4.11 | *Packet-Delay Variation*

Fonte: elaborada pelo autor.

Caro aluno, para compreensão da Figura 4.11, observe o esquema a seguir:

1. O pacote transmitido pelo Servidor, no tempo 1, é recebido no período certo pelo Cliente.

2. O pacote enviado pelo Servidor no Tempo 2 tem sua ordem trocada e chega ao Cliente no Tempo 5.

3. O pacote enviado pelo Servidor no Tempo 3 tem sua ordem trocada e chega ao Cliente no Tempo 4.

Para que as mensagens trocadas entre os dispositivos possam chegar ao seu destino, são necessários protocolos, equipamentos, meios de transmissão, entre outras coisas.

Quando os pacotes são transmitidos e chegam em ordem trocada (*jitter*), podemos considerá-los como perdidos, assim como ocorre na perda de pacotes?

Disponibilidade

Segundo Comer (2007), as redes de computadores são compostas por diversos equipamentos, como nodos, computadores, servidores, cabeamentos, entre outros, cada um dos quais é um sistema suscetível a falhas. Ou seja, é a descrição da capacidade que equipamentos e redes possuem de forma contínua (sem que haja interrupção), por um período.

Caro aluno, na Seção 4.2 você estudou dois conceitos, entre eles:

- Tempo médio entre falhas (MTBF – *mean time between failures*): é uma previsão por modelo estatístico/matemático do tempo médio entre as falhas. É útil para os profissionais de tecnologia da informação para prever as manutenções necessárias. Para o cálculo, utiliza-se:

$$MTBF = \frac{\sum(Final - Início)}{Número\ de\ falhas}$$

- Tempo médio para reparos (MTTR – *mean time to repair*): é uma previsão por modelo estatístico/matemático do tempo médio para efetuar reparo após a ocorrência de falha. Para o cálculo, utiliza-se:

$$MTTR = \frac{Tempo\ parado\ por\ falha}{Número\ de\ falhas}$$

Para que seja possível calcular a disponibilidade, é necessário compreender o tempo médio para falha (MTTF – *mean time to failure*): tempo de vida de uma rede que compreende os períodos alternados de operação de falhas.

Com isso, é possível efetuar o cálculo de disponibilidade, por meio da função de frequência com que as falhas ocorrem e o tempo necessário para reparo, em que:

$$D = MTTF / (MTTF + MTTR)$$

Para exemplificarmos uma aplicação, imagine que uma rede possua um MTTF de 8.000 horas de operação anual e um MTTR de 36 horas anual. Nesse caso:

$$D = 8000 / (8000 + 36)$$

$$D = 99,5$$

Ou seja, a disponibilidade da rede é de 99,5% ao ano.

Pesquise mais

O software Iperf permite realizar algumas medições nas redes a fim de se conhecer mais sobre a estrutura. O trabalho intitulado *Análise de impacto na transição entre os protocolos de comunicação IPv4 e IPv6*, de Nunes (2013), demonstra uma comparação de latência, *throughput, jitter* e perda de pacotes em uma rede IPv4 pura, IPv6 pura e pilha dupla.

Disponível em: <http://repositorio.unicamp.br/jspui/handle/REPOSIP/267748>. Acesso em: 29 jul. 2017.

QoS (*Quality of Service* – Qualidade de Serviço)

Segundo Tanenbaum (1997), qualidade de serviço em redes de computadores pode ser definida como um conjunto de regras, mecanismos e tecnologias que tem o propósito de utilizar os recursos disponíveis de forma eficaz e econômica. Além disso, os fatores que determinam diretamente a qualidade de transmissão são: latência, *jitter*, perda de pacotes e largura de banda disponível.

Para que sejam atendidas às necessidades das redes, são utilizados dois modelos de QoS, entre os quais temos:

- IntServ: utiliza o fluxo dos dados por meio do protocolo no caminho que a mensagem deve percorrer. Possui serviço garantido no envio/recebimento de mensagens fim a fim e o controle (balanceamento) de carga.
- DiffServ: conhecido como serviços diferenciados, trata-se de uma marcação no pacote para classificá-los e efetuar os tratamentos necessários de forma independente. Este modelo é altamente adotado por fabricantes de equipamentos IPv6.

Qualidade dos serviços, disponibilidade, capacidade de processamento e armazenamento do provedor de serviços são

determinados pelo SLA (*service level agreement* – acordo de nível de serviço). Este tem como função especificar os níveis de desempenho em contrato de serviço.

Caro aluno, as configurações de equipamentos como computadores, roteadores, *switchs*, impressoras, entre outros, dependem de algumas características, como:

- Serviços: as configurações de equipamentos dependem do tipo de serviço que está sendo utilizado na rede, por exemplo, VoIP, videoconferência, aplicações web, etc.
- Dispositivos: existem diversos tipos de fabricantes de equipamentos (roteador, *switch*, servidor, etc.), cada um com uma forma própria para configuração, capacidade de processamento, suporte e demais características técnicas.

Um exemplo de configuração de equipamentos é a utilização do VLAN Trunk Protocol. Trata-se de um protocolo de camada 2, desenvolvido pela Cisco, para configuração de VLANs, facilitando, assim, a sua administração. Mas o que é uma VLAN?

Fillippetti (2008) mostra que VLAN é definida como rede local virtual (*virtual lan network*). Trata-se de uma maneira de criar sub-redes de forma virtual. Se feita em *switchs*, cada uma das interfaces pode ser uma VLAN e ter o seu próprio domínio de broadcast. Observe o exemplo na Figura 4.12:

Figura 4.12 | *Packet-Delay Variation*

Fonte: elaborada pelo autor.

Basicamente, o VTP (VLAN *Trunk Protocol*) cria uma estrutura do tipo cliente-servidor, em que as alterações obrigatoriamente são feitas no servidor, que, por sua vez, posteriormente as replica aos clientes. Tal técnica é largamente utilizada pelos administradores de redes.

Caro estudante, ao discutirmos os assuntos abordados nesta seção de aprendizagem, podemos compreender alguns parâmetros que devem ser observados pelos administradores de redes para que se possam garantir a qualidade dos serviços e a disponibilidade da rede. Além disso, pode-se compreender também a forma pela qual a configuração e a padronização de procedimentos podem auxiliar os profissionais de tecnologia da informação, no gerenciamento das redes de computadores.

Sem medo de errar

A T2@T Visão, empresa que produz armação para óculos, recentemente firmou parcerias em cujos contratos determina que a base de dados deve permanecer disponível mais que 90% do tempo para que se evite pagar multa.

A rede tem um MTTF de 8.000 horas. Segundo cálculos anteriores, todos os dias o serviço fica indisponível por uma hora. Dessa forma, segue o relatório:

Sr. Gerente da T2@T Visão,

O servidor trabalha anualmente 8.000 horas.

O tempo necessário para efetuar a manutenção e a correção de falhas é de uma hora por dia (24 horas).

Seguem os cálculos:

$$MTTR = 1\ hora * 365\ dias$$

$$MTTR = 365\ horas$$

$$D = MTTF\ /\ (MTTF + MTTR)$$

$$D = 8000\ /\ (8000 + 365)$$

$$D = 0,9563$$

Dessa forma, podemos concluir que a disponibilidade da rede é de 95,63% ao ano, ou, ainda 7.650 horas, aproximadamente. Tal cenário tem uma folga de 5,63% da capacidade do servidor, sendo desnecessário, no momento, fazer alterações na infraestrutura para atender aos contratos.

Avançando na prática

Provedor de internet

Descrição da situação-problema

A empresa 8909_NET provê serviço de internet na cidade de Nerdópolis. A maior parte dos seus habitantes possui um dos pacotes de serviço, porém a região sul da cidade ainda não tem a infraestrutura completa para que o serviço seja oferecido.

Você foi contratado para o projeto de expansão da 8909_NET. Para que possa ser planejado o aumento de clientes, o gerente designou que você efetue o cálculo de disponibilidade. Para isso, ele deseja saber o tempo de manutenção (MTTR) anual para disponibilidade de aproximadamente 95%. Leve em consideração que o MTTF da rede é de 7.200 horas anuais.

Resolução da situação-problema

Para que a 8909_NET possa planejar o aumento da sua rede, a fim de expandir a sua infraestrutura na cidade de Nerdópolis, o gerente designou que você efetuasse o cálculo de disponibilidade de serviços.

Levando em consideração o MTTF de 7.200 horas anuais, ele deseja saber o tempo de manutenção anual (MTTR) para uma disponibilidade de aproximadamente 95%. Segue relatório:

Sr. Gerente,

Para disponibilidade de 95%, temos que:

$$MTTR = ?$$

$$D = 0,95$$

$$MTTF = 7200$$

$$D = MTTF / (MTTF + MTTR)$$

$$0,95 = 7200 / (7200 + MTTR)$$

$$0,95 * (7200 + MTTR) = 7200$$

$$0,95 MTTR = 7200 - 6840$$

$$MTTR = \frac{360}{0,95}$$

$$MTTR = 378$$

Portanto, a rede pode ficar indisponível 378 horas por ano.

Faça valer a pena

1. O Brasil está entre os cinco maiores consumidores de jogos eletrônicos e internet do mundo. Parece que essa combinação conquistou boa parte dos jovens. Por esse motivo, os títulos de jogos on-line estão entre aqueles mais consumidos, com destaque para:

- PES.
- Battlefield.
- FIFA.
- Call of Duty.
- Counter Strike.

Fonte: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/brasil-e-o-4-consumidor-de-games-mas-mercado-carece-de-mao-de-obra.html>. Acesso em: 7 ago. 2017.

Os jogos podem ser utilizados em videogames ou por computador, o que pode variar conforme a preferência do *gamer*.
Algumas ocorrências durante a transmissão podem degradar as partidas on-line, fazendo com que ocorram:

- Travamento da movimentação do personagem do jogo.
- Movimento estranho ou inesperado do personagem do jogo.
- Banimento da sala por conexão ruim.
- Perda de conexão.

Um dos motivos da degradação dos serviços pode ser expresso como:
X = *Tempo de transmissão + Tempo de propagação*

Assinale a alternativa que substitua a variável "X" da expressão, corretamente:
a) Perda de pacotes.
b) Latência.
c) *Jitter*.
d) *throughput*.
e) QoS.

2. A videoconferência é um serviço largamente utilizado pelas empresas, pois permite que as pessoas se comuniquem por longas distâncias, fazendo chamadas de áudio e vídeo. A qualidade desse tipo de serviço vai depender de uma rede com boa vazão, ausência de jitter, baixa latência e perda de pacotes.
Existem vários softwares e aplicações web utilizados para esse fim, entre os quais podem se destacar:
• Messenger.
• Skype.
• GroupChat.
• Talk.
• Socialeyes.
Todos esses produtos são softwares gratuitos que podem ser utilizados para comunicação.

Para verificar os travamentos que estavam ocorrendo nas chamadas de videoconferência, um administrador de redes efetuou o seguinte teste:

Teste de rede

```
Disparando 192.168.0.1 com 32 bytes de dados:
Resposta de 192.168.0.1: bytes=32 tempo=3ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=3ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=4ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=410ms TTL=64
Esgotado o tempo limite do pedido.
Resposta de 192.168.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=8ms TTL=64

Estatísticas do Ping para 192.168.0.1:
    Pacotes: Enviados = 10, Recebidos = 9, Perdidos = 1 (10% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1ms, Máximo = 410ms, Média = 48ms
```

Fonte: elaborada pelo autor.

Com base na figura, observe as afirmativas a seguir:
I. Foram enviados 10 pacotes, dos quais 9 foram recebidos e 1 foi perdido.
II. O *jitter* ocorreu no oitavo pacote enviado.
III. A latência média foi de 48 ms.

Assinale a alternativa correta:
a) Somente as afirmativas I e II são verdadeiras.
b) Somente as afirmativas II e III são verdadeiras.
c) Somente as afirmativas I e III são verdadeiras.
d) Somente as afirmativas I, II e III são verdadeiras.
e) Somente a afirmativa I é verdadeira.

3. Quando inicia um projeto de estruturação de topologia, o administrador de redes deve estar atento a vários fatores:
• Cabeamento estruturado.
• Equipamentos como nodos, servidores, etc.
• Segurança.
• Controle de acesso.
• Entre diversas outras necessidades.
Na fase de configuração dos equipamentos, alguns fabricantes disponibilizam algumas ferramentas a fim de agregar qualidade e eficiência no gerenciamento de alguns serviços.

Sempre que o administrador de redes necessita fazer alteração em um switch para configurar uma VLAN, os demais switchs conectados em uma das suas interfaces também necessitam de algumas alterações.
Para que as configurações, alterações e demais atividades relacionadas às VLANs da rede possam ocorrer de forma mais eficiente, é preciso utilizar:

a) VLAN Analyser.
b) VLAN Unique Protocol.
c) Trunk Protocol Virtual.
d) Virtual VLAN Protocol.
e) VLAN Trunk Protocol.

Referências

CARISSIMI, A. **Redes de computadores**. Instituto de Informática UFRGS. Porto Alegre: Bookman, 2009.

COMER, D. E. ***Computer and networks internet with internet applications***. São Paulo: Artmed, 2007.

FILIPPETTI, M. A. **CCNA 4.1**: Guia completo de estudos. Florianópolis: Visual Books, 2008.

FOROUZAN, A. **Comunicação de dados e redes de computadores**. Porto Alegre: Bookman, 2006.

G1. **Brasil é o 4º consumidor de games, mas mercado carece de mão de obra**. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/brasil-e-o-4-consumidor-de-games-mas-mercado-carece-de-mao-de-obra.html>. Acesso em: 27 nov. 2017.

KUROSE, J. F. **Redes de computadores e a internet:** uma abordagem top-down. 3. ed. São Paulo: Pearson, 2006.

TANENBAUM, A. S. **Redes de computadores**. 4 ed. Rio de Janeiro: Campus, 1997.

WORD REFERENCE. **Sniff.** Disponível em: <http://www.wordreference.com/es/translation.asp?tranword=sniff> Acesso em: 27 nov. 2017.